GUIDE

Stormshield Network

REALTIME MONITOR V.1.2 USER CONFIGURATION MANUAL

Date	Details
May 2014	Creation
September 2014	Update
November 2014	Update

Reference: snengde_snrmonitor-v1.2

FOREWORD

License

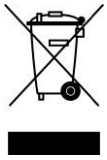
Products concerned

U30, U70, U120, U250, U450, U1100, U1500, U6000,
NG1000-A, NG5000-A,
U30S, U70S, U150S, U250S, U500S, U800S,
SN150, SN200, SN300,
SN500, SN700, SN900,
SN2000, SN3000, SN6000,
VS5, VS10, V50, V100, V200, V500 and VU.

Liability

This manual has undergone several revisions to ensure that the information in it is as accurate as possible. The descriptions and procedures herein are correct where Stormshield Network firewalls are concerned. NETASQ rejects all liability directly or indirectly caused by errors or omissions in the manual as well as for inconsistencies between the product and the manual.

Notice



WEEE Directive

All NETASQ products that are subject to the WEEE directive will be marked with the mandated "crossed-out wheeled bin" symbol (as shown above) for items shipped on or after August 13, 2005. This symbol means that the product meets the requirements laid down by the WEEE directive with regards to the destruction and reuse of waste electrical and electronic equipment.

For further details, please refer to the website at this address:

http://www.netasq.com/recycling.html

CONTENT

1. INTRODUCTION 7
1.1 BASIC PRINCIPLES 7
1.1.1 WHO SHOULD READ THIS? 7
1.1.2 TYPOGRAPHICAL CONVENTIONS 7
1.1.3 VOCABULARY USED IN THE MANUAL 9
1.1.4 GETTING HELP 9
1.1.5 TECHNICAL ASSISTANCE CENTRE 9
1.2 SOFTWARE INSTALLATION 9
1.2.1 PRE-REQUISITES 10
1.2.2 INSTALLING VIA YOUR PRIVATE AREA 11
2 SN REALTIME MONITOR 12
2.1 CONNECTION 12
2.1.1 Access 12
2.1.2 Connection 13
2.1.3 Address book 15
2.2 GETTING FAMILIAR WITH REAL-TIME MONITOR 19
2.2.1 PRESENTATION OF THE INTERFACE 19
2.2.2 INTRODUCTION TO MENUS 40
2.2.3 APPLICATION SETTINGS 41
2.2.4 DEFAULT MONITORING SETTINGS 45
3 INFORMATION ON FIREWALLS 47
3.1 OVERVIEW 47
3.1.1 Introduction 47
3.1.2 Overview of information on vulnerabilities 48
3.1.3 List of firewalls 48
3.1.4 Connection logs 49
3.2 DASHBOARD 49
3.2.1 Introduction 49
3.2.2 Selecting a product 51
3.2.3 System information 51
3.2.4 Memory 51
3.2.5 CPU 52
3.2.6 Temperature 52
3.2.7 Hardware 52
3.2.8 Active network policies 53
3.2.9 Alarms 53
3.2.10 Vulnerabilities 53
3.2.11 VPN Tunnels 53
3.2.12 Active Update 53
3.2.13 Logs 53
3.2.14 Services 54
3.2.15 Proxy Cache 54
3.2.16 Interfaces 54
3.2.17 Top 5 interfaces for incoming throughput 54
3.2.18 Top 5 interfaces for outgoing throughput 54
3.2.19 Top 5 hosts for incoming throughput 54
3.2.20 Top 5 hosts for outgoing throughput 54
4 REAL-TIME INFORMATION 55
4.1 EVENTS 55
4.2 SN Vulnerability Manager (NVM) 58
4.2.1 Introduction 58
4.2.2 Vulnerabilities tab 59
4.2.3 Application tab 61
4.2.4 Events tab 63
4.3 HOSTS 65
4.3.1 "Hosts" tab 65
4.3.2 "DHCP leases" tab 71
4.4 INTERFACES 71
4.4.1 Introduction 71
4.4.2 Legend view (or tabular view of interfaces) 73
4.4.3 "Details" view 73
4.4.4 "Bandwidth" tab 74
4.4.5 "Connections" tab 74
4.4.6 "Incoming connections" tab 75
4.4.7 "Outgoing connections" tab 75
4.4.8 "Throughput" tab 75
4.5 QUALITY OF SERVICE (QoS) 76
4.5.1 "Diagram" view 77
4.5.2 "Connections" view 77
4.6 USERS 77
4.6.1 Introduction 77
4.7 QUARANTINE – ASQ BYPASS 78
4.7.1 "Quarantine" view 79
4.7.2 "ASQ Bypass" view 79
5 NETWORK ACTIVITY 80
5.1 VPN TUNNELS 80
5.1.1 IPSec VPN Tunnels tab 80
5.1.2 SSL VPN Tunnels tab 82
5.2 ACTIVE UPDATE 83
5.3 SERVICES 84
5.4 HARDWARE 85
5.4.1 High availability 85
5.4.2 Power supplies 85
5.4.3 S.M.A.R.T. devices 85
5.4.4 RAID 86
5.4.5 Log Storage Disks 86
6 POLICIES 87
6.1 FILTER POLICY 87
6.2 VPN POLICY 87
7 LOGS 89
7.1 STATUS OF USE 89
7.2 LOG TYPES 89
7.2.1 VPN 89
7.2.2 System 90

1. INTRODUCTION

1.1 BASIC PRINCIPLES

1.1.1 WHO SHOULD READ THIS?

This manual is intended for network administrators or, at the least, for users with IP knowledge.

In order to configure your Stormshield Network UTM firewall in the most efficient manner, you must be familiar with IP operation, its protocols and their specific features:

- ICMP (*Internet Control Message Protocol*)
- IP (*Internet Protocol*)
- TCP (*Transmission Control Protocol*)
- UDP (*User Datagram Protocol*)

Knowledge of the general operation of the major TCP/IP services is also desirable:

- HTTP
- FTP
- Mail (SMTP, POP3, IMAP)
- Telnet
- DNS
- DHCP
- SNMP
- NTP

If you do not possess this knowledge, don't worry: any general book on TCP/IP can provide you with the required elements.

The better your knowledge of TCP/IP, the more efficient your filter rules and the greater your IP security.

1.1.2 TYPOGRAPHICAL CONVENTIONS

1.1.2.1 Abbreviations

For the sake of clarity, the usual abbreviations have been kept. For example, **VPN** (*Virtual Private Network*).

1.1.2.2 Display

Names of windows, menus, sub-menus, buttons and options in the application will be represented in the following fonts:

Example

Menu **Interfaces**

1.1.2.3 Indications

Indications in this manual provide important information and are intended to attract your attention. Among these, you will find:

NOTE/REMARKS

These messages provide a more detailed explanation on a particular point.

WARNING/RECOMMENDATION

These messages warn you about the risks involved in performing a certain manipulation or about how not to use your appliance.

TIP

This message gives you ingenious ideas on using the options on your product.

DEFINITION

Describes technical terms relating to Stormshield Network or networking. These terms will also be covered in the glossary.

1.1.2.4 Messages

Messages that appear in the application are indicated in double quotes.

Example

"Delete this entry?"

1.1.2.5 Examples

Example

This allows you to have an example of a procedure explained earlier.

1.1.2.6 Command lines

Command lines

`Indicates a command line (for example, an entry in the DOS command window).`

1.1.2.7 Reminders

Reminders are indicated as follows:

- Reminder.

1.1.2.8 Access to features

Access paths to features are indicated as follows:

- Access the menu **File\Firewall.**

1.1.3 VOCABULARY USED IN THE MANUAL

Appliance	Refers to the security device (firewall). The terms "appliance" and "security device" are used interchangeably.
Dialup	Interface on which the modem is connected.
Firewall	Stormshield Network UTM device /product
Intrusion prevention	Unified Threat Management is also used in its place.
Configuration slot	(or *policy*). Configuration files which allow generating filter and NAT policies, for example.
Host	Terms used as much to refer to workstations as to users.
Logs	A record of user activity for the purpose of analyzing network activity.

1.1.4 GETTING HELP

To obtain help regarding your product and the different applications in it:

- website: https://mystormshield.eu/. Your secure-access area allows you to access a wide range of documentation and other information.
- user manuals: Stormshield Network UNIFIED MANAGER, Stormshield Network REAL-TIME and Stormshield Network EVENT REPORTER.

1.1.5 TECHNICAL ASSISTANCE CENTRE

Stormshield Network provides several means and tools for resolving technical problems on your firewall.

- A knowledge base.
- A certified distribution network. As such, you will be able to call on your distributor.
- Documents: these can be accessed from your client or partner area. You will need a client account in order to access these documents.

For further information regarding technical assistance, please refer to the document "Support charter".

1.2 SOFTWARE INSTALLATION

This section provides you with the elements for installing the software suite that would allow you to administer your product. *For further information on the appliances and how to*

install them, please refer to the product installation guide "Presentation and installation of Stormshield Network *products", (Ref. naengde_product-installation.pdf).*

You will need the graphical interface installation file. This file can be found on the website (https://mystormshield.eu/). The installation file is in English and French. You will also need your firewall's internal IP address as well as its serial number.

1.2.1 PRE-REQUISITES

The basic library corresponds to all the modules necessary for the other programs. 15.3 MB of hard disk space is necessary.

The minimum installation groups together:

- Stormshield Network Unified Manager: Graphical interface for the administration of Stormshield Network Firewalls
- Stormshield Network Real-Time Monitor: Real-time viewer of your Stormshield Network Firewall (2.58 MB)
- Stormshield Network Event Reporter: Log consultation and management on your firewall (140 MB)

The installation comprises all the graphic configuration tools of the Stormshield Network suite, which serve as the interface between the user and the appliance. These tools have to be installed on an administration workstation.

The Stormshield Network Firewall is fully configured via a software program developed by NETASQ – Stormshield Network UNIFIED MANAGER. Using this program, you will be able to configure your firewall from a Windows workstation.

You will need the following elements in order to install this software:

- CPU with a minimum of 2GHz
- A minimum of 2 GB of RAM (Windows 7) for client software, 2 GB for server software.
- About 300MB of hard disk space as this is what the software will occupy after its installation. If possible, reserve several gigabytes of space for the database (depending on the activity of the connected firewall(s).
- Ethernet 100 or 1000 Mbps network card

Software applications are supported on the following operating systems:

- Microsoft Windows 7 and 8,
- Microsoft Windows Server 2008 and 2012.

1.2.2 INSTALLING VIA YOUR PRIVATE AREA

Download the necessary files from the website and execute the .EXE program corresponding to the administration suite. The installation information will appear in the same language as the version of Windows that has been installed.

1.2.2.1 Verification procedure

1.2.2.1.1 Signature verification procedure

When you download an application from your client or partner area on https://mystormshield.eu/, the following message will appear: "Open a file or save on your computer?"

- If you choose "Open", your web browser will check the signature automatically and inform you about the results.
- If you choose "Save" (recommended option), you will need to perform the check manually.

-

1.2.2.1.2 Manual verification

To manually check the application's signature, follow the procedure below before installing the application:

1. Right-click on the Stormshield Network appliance whose signature you wish to check then select the menu **Properties** from the contextual menu that appears.
2. Select the **Digital signatures** tab then the name of the signor (NETASQ).
3. Click on **Details**: this window will indicate whether the digital signature is valid.

1.2.2.2 Registration

During installation, you will be asked to register your product. This registration is mandatory in order to obtain your product's license, to download updates and to access technical support.

2 SN REALTIME MONITOR

Stormshield Network REAL-TIME MONITOR allows you to visualize your Firewall's activity in real time and provides the information below:

- Use of the Firewall's internal resources (memory, CPU, etc.),
- List of raised alarms when vulnerabilities are detected
- List of connected hosts and users,
- Real-time alarms,
- Number of connections, bandwidth use, throughput,
- Information on the status of interfaces and VPN tunnels,
- Last logs generated,
- Use of disk space allocated to logs.

With this tool, you can connect to several Firewalls and supervise all of them.

Stormshield Network REAL-TIME MONITOR provides a simple display of connections transiting via the Firewall, along with any alarms it has generated.

Monitor can be shut down by clicking on the cross in the top right corner, but this does not stop it from operating. Clicking on the Monitor icon in the taskbar restores it.

By default, Monitor can only be run on a machine connected to the internal network and must be running permanently in order to avoid missing any alarms. You can use it remotely (through the internet) but you would have to explicitly authorize the service (Firewall_srv) in the filter rules.

2.1 CONNECTION

2.1.1 Access

There are 2 ways to launch the **Stormshield Network REAL-TIME MONITOR** application:

- Via the shortcut **`Applications\Launch the REAL-TIME-MONITOR`** in the menu bar on other applications in the Administration Suite.
- Via the menu **`Start\Programs\Stormshield\Administration Suite 1.0\Stormshield Network REAL-TIME MONITOR.`**

If this is your very first time connecting to your product, a message will prompt you to confirm the serial number (found on the underside of the firewall).

The **Overview** window will open upon connection:

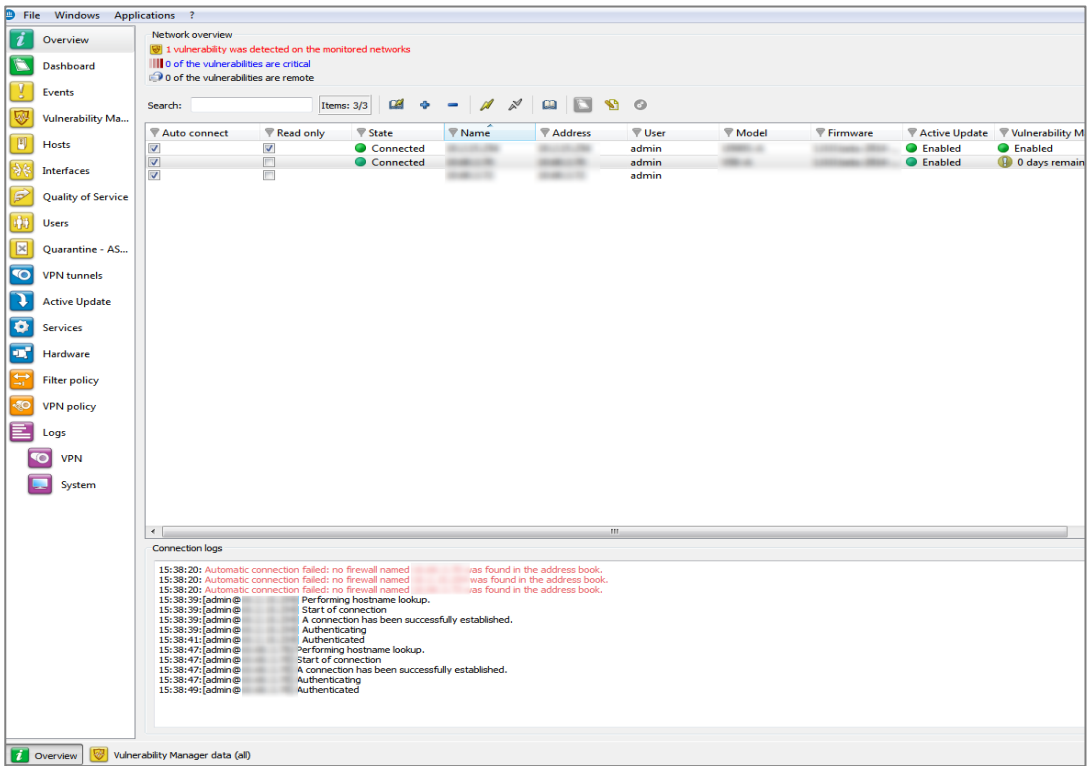


Figure 1: Overview

2.1.2 Connection

Stormshield Network REAL-TIME MONITOR is opened differently depending on the option chosen in the tab **Startup behavior** in **Application settings** (cf. Part 2/Chapter *Startup behavior*).

The possible options are:

- Direct connection
- Connect to automatic connection data sources
- None

2.1.2.1 Direct connection to a Stormshield Network multifunction Firewall

Direct connection allows you to enter connection information for a specific firewall.

To make a direct connection, go to the menu **File\Direct connection.** Or, if Monitor has been configured to connect directly at startup, the following window will appear:

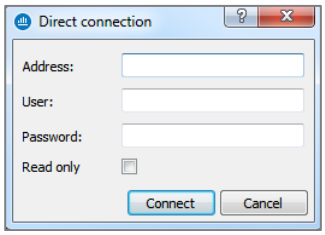


Figure 2: Direct connection

NOTE

For more information regarding connection, please refer to Part 2/Chapter *Startup behavior*.

1. Indicate the firewall's IP address in the **Address** field.
2. Enter the administrator login in the **User** field.
3. Enter the administrator password in the **Password** field.

REMARK

Select the option **Read only** to connect to the firewall in read-only mode.

4. Click on the **Connect** button. The main window will appear.

2.1.2.2 Opening the address book

Go to the menu **File\Address book** to open the address book. Or, if Monitor has been configured to open the address book at startup, the Address book window will appear:

NOTE

For more information regarding the address book, please refer to *Part2/Chapter Address book.*

2.1.2.3 Connecting automatically to the data source

If this option has been selected in **Startup behavior\Application settings**, Monitor will directly open the "Overview" main window and the application will automatically connect to the existing firewalls. (*cf. for more information regarding connection, please refer to the section* Part 2/Chapter *Startup behavior*.)

2.1.2.4 None

If this option has been selected in **Startup behavior\ Application settings**, Monitor will directly open the "Overview" main window but no application will be connected to the firewall. Only the **Overview** menu will be enabled. The other menus in the directory will be grayed out. (*cf. for more information regarding connection, please refer to* Part 2/Chapter *Startup behavior)*

2.1.3 Address book

The address book can be accessed from the menu **File\Address book.**

REMARK

The address book can also be opened automatically upon the startup of the application if you have selected the option in **Application settings/Behavior at start up** (*See* Part 2/Chapter *Startup behavior*).

It is possible to store connection data on your different Firewalls. This information is stored on the same client workstation on which the interface has been installed. It may be encrypted if you check the option **Address book is encrypted**. In this case, you will be asked to enter an encryption key. The information that is stored for each firewall includes the IP address, login name, connection password and the serial number of the Firewall to which you wish to connect. This password belongs to an authorized user.

By specifying a serial number, you will protect yourself from "man-in-the-middle" attacks. If you attempt a connection on a firewall that does not meet the "serial number" criterion indicated in the address book, the monitor will inform you that you are attempting to connect to an unknown firewall. You will also be asked if you wish to add this serial number to the list of authorized firewalls. Verify the information displayed in the monitor before accepting such a request.

Once this information has been entered, you may save it using the **Save** button. To open a session on one of the Firewalls from the address book, click on its name then on the **OK** button, or simply double click on the name of the Firewall.

WARNING

If you modify the **Address book is encrypted** option, the address book has to be saved once more to apply the changes

Check the option **Display passwords** to check the passwords used for each Firewall saved in the address book (passwords are displayed in plaintext).

2.1.3.1 Adding an address

Click on the **Add** button to add an address to the address book. Other information to supply:

Name	The name of the firewall
Address	IP address of the firewall
Login	The administrator account.
Password	Administrator password
Confirm	Confirms the password
Description	Description or comments regarding the firewall.

2.1.3.2 Modifying an address

The procedure for modifying an address in the address book is as follows:

1. Select the firewall to be modified.
2. Click on the **Modify** button. The following window will appear:

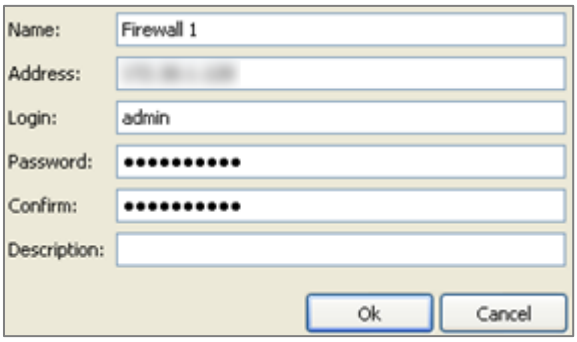


Figure 3: Modifying an address

3 Make the necessary changes.

4 Click on **OK** to confirm changes.

2.1.3.3 Deleting an address

The procedure for deleting a firewall from the address book is as follows:

1 Select the firewall to delete.

2 Click on the **Delete** button. The following message will appear: "Confirm deletion of these items?"

3 Click on **Yes** or **No** to confirm deletion or cancel.

2.1.3.4 Importing an address book

The procedure for importing an existing address book is as follows:

1 Click on the **Import** button. The following window will appear:

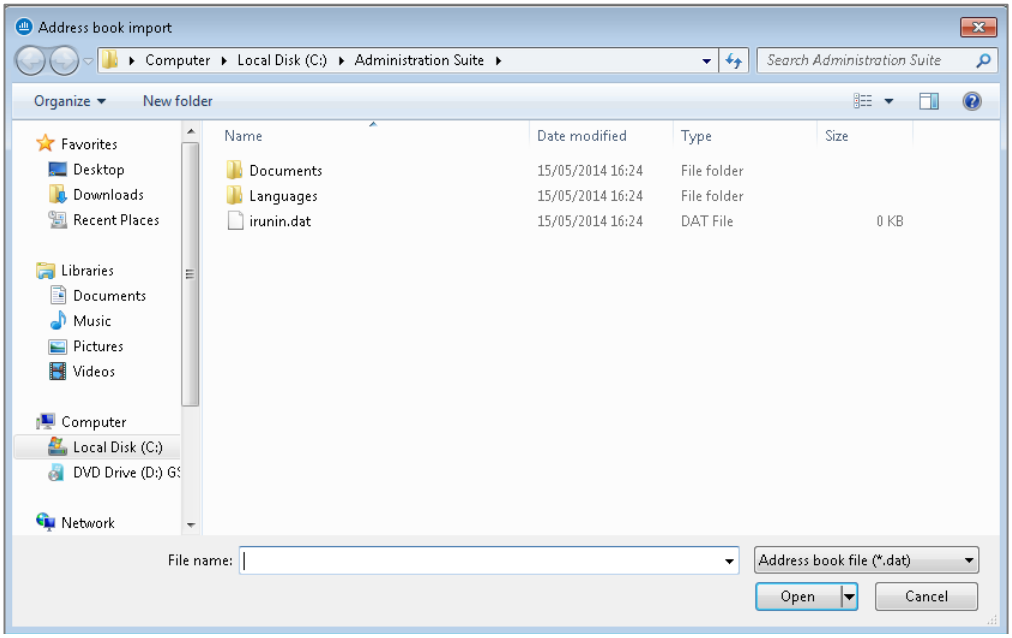


Figure 4: Importing the address book

2 Select the file to import.

REMARK

The file to import should be in **.dat** format.

3 Click on **Open**.

2.1.3.5 Exporting an address book

The procedure for exporting an existing address book is as follows:

1 Click on **Export**. The following window will appear:

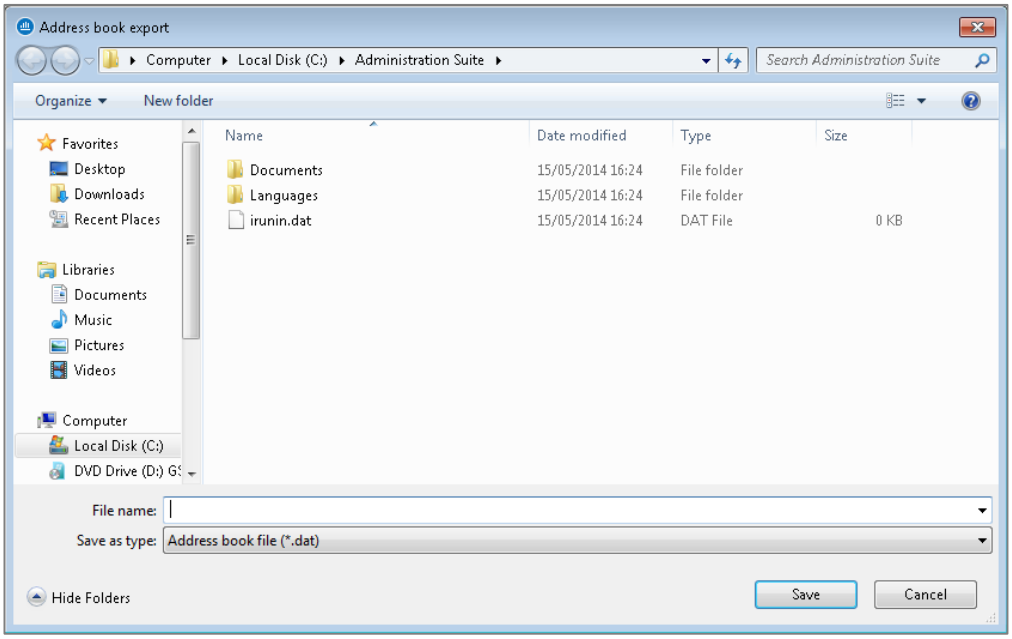


Figure 5: Exporting the address book

2 Select the file to export.

REMARK

The file to export should be in **.dat** format.

3 Click on **Save**.

2.1.3.6 Search

The search covers all information found in the columns.
Information can be filtered on a column and the search can then be refined.

Examples:

- Filter on the "Address" column containing 129: a list of results will appear; next, launch a global search by refining according to address.
- Filter on the "Address" column beginning with "10.2", then search from the displayed addresses, hosts with addresses beginning with "10.2.14" by entering only "14" in the search field.

2.2 GETTING FAMILIAR WITH REAL-TIME MONITOR

2.2.1 PRESENTATION OF THE INTERFACE

2.2.1.1 Main window

From this window, you can open several windows, each connected to different firewalls.

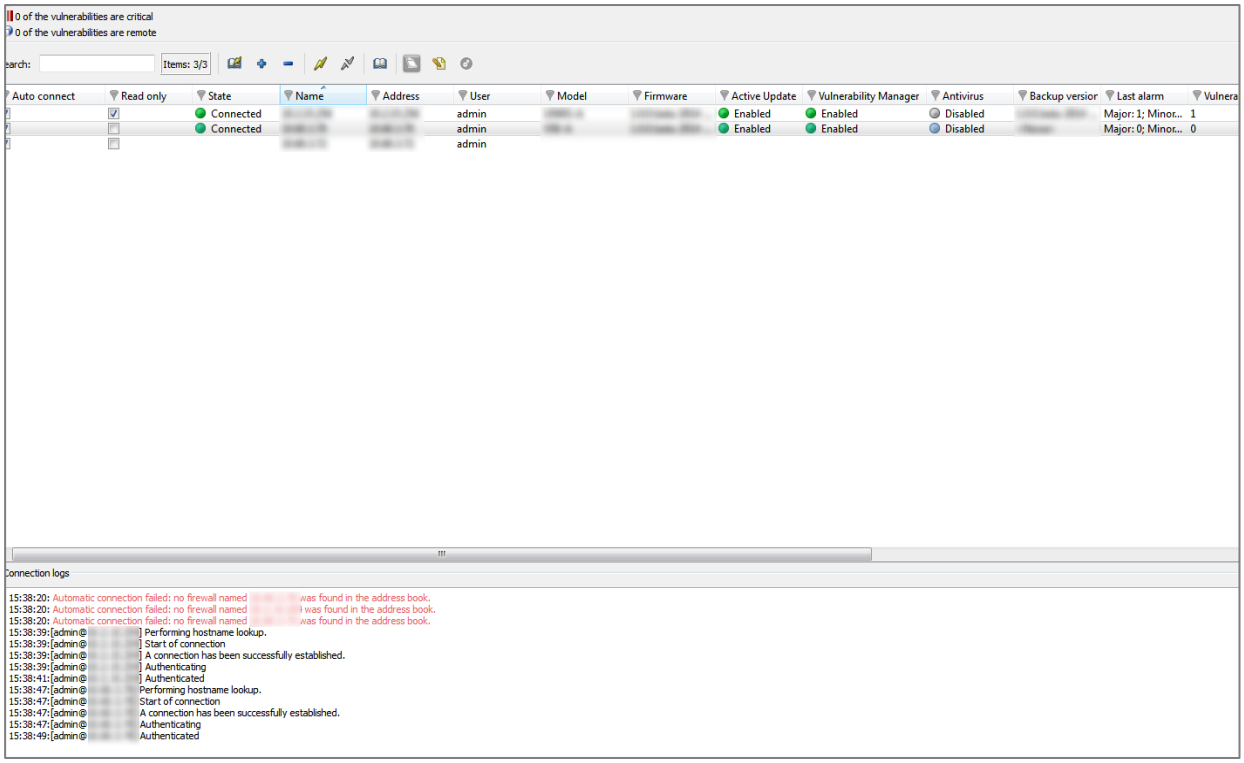


Figure 6: Overview

Once Monitor is connected, it will open a welcome window (**Overview** Menu) which will display various types of information on the firewall's activity.

It consists of five parts:

- A menu bar
- A horizontal bar containing icons relating to connection and a search zone
- A vertical bar containing a menu directory allowing **Stormshield Network REAL-TIME MONITOR** options to be viewed and configured
- A result display zone
- A status bar

REMARK

The other windows in the menu directory may contain the following buttons:

- Refresh
- Show/Hide help
- Firewall
- Duplicate

2.2.1.2 Description of icon

	Connects via the address book.
	Connects to a firewall
	Disconnects or deletes a connection.
	Connects to the selected firewall.
	Disconnects from the selected firewall.
	Edits the address book address book.
	Displays the dashboard of the selected firewall.
	Generates a web report for the selected firewall: • Summary of system resources, memory, CPU, etc. • List of connected hosts (IP address, interface to which the user is connected, amount of data transferred, number of connections, throughput used...). • List of authenticated users (user name, IP, remaining time on authentication period...). • List of alarms raised (major and minor). • List of active VPN tunnels. • List of active services. • Status of the Active Update module. • Statistics. • Vulnerability Manager…
	Logs on to the selected firewall's web administration.

2.2.1.3 Menus

The main window contains the following menus: **File**, **Windows**, **Applications**, and **? (Help)**.

File	Allows you to connect to Firewalls and to access the application's general options.
Windows	Allows you to organize the connection windows on the screen.
Applications	Enables you to execute the two other applications making up the Stormshield Network Administration Suite: Stormshield Network UNIFIED MANAGER et Stormshield Network EVENT REPORTER.
? (Help)	Allows you to access the relevant Help file, and to know which version the monitor runs on.

2.2.1.4 Menu directory

Overview	This window lists the firewalls. Monitor opens in this window once the connection has been established... The Console sub-menu: When the option Enable is selected in the menu `Application parameters\Miscellaneous` in the console zone, you will be able to access firewalls in console mode (CLI commands). When this window

	is validated, a `Console` menu will be added under the `Overview` menu directory.
Dashboard	This window gives you a summary of the main information relating to your product's activity.
Events	This window lists events that the firewall has raised.
Vulnerability Manager	This window allows you to view alarms being raised and to get help in the event of vulnerability.
Hosts	List of hosts on your network.
Interfaces	This window allows you to get statistics on bandwidth, connections and throughput.
Quality of service	This window allows you to analyze your bandwidth, connections and throughput.
Users	This window allows you to get information on users and session privileges on authentication.
Quarantine - ASQ Bypass	This window displays the list of dynamically quarantined hosts.
VPN Tunnels	This window displays static information on the operation of VPN tunnels and on the source and destination.
Active Update	This window sets out the status of Active Update on the firewall for each type of update available.
Services	This window shows the active and inactive services on the firewall and how long they have been active/inactive.
Hardware	This window shows information on the initialization of high availability and RAID.
Filter policy	This window displays the active filter policy by grouping the implicit and local rules.
VPN policy	This window allows viewing the configuration of different VPN tunnel policies.
Logs	This window allows viewing in real time the size of the log file. • The sub-menu VPN provides information on VPN logs. • The sub-menu System provides system information.

2.2.1.5 Result display zone

Data and options from the selected menus in the horizontal bar appear in this zone. These windows will be explained in further detail in the corresponding sections.

2.2.1.5.1 Contextual menu on columns

Right-clicking on a column header will display the following options

Filter by this column…	Isolates a set of events according to the criteria provided. For example, filtering by events with a "minor" protocol. When a filter has been applied to a column, the icon will appear in blue in the column label.
Clear column filter	Removes the filter that was previously set on the column.
Clear all filters	Removes the filters set on all the columns.
Clear all filters except this	Removes the filters set on all the columns except for the filter on the selected column.
Hide column	Hides the selected column.
Columns	Allows selecting the columns to display.

Adjust column width to fit contents	Columns will be resized according to the contents.

When the menu **`Filter by this column`** is selected, the following screen will appear:

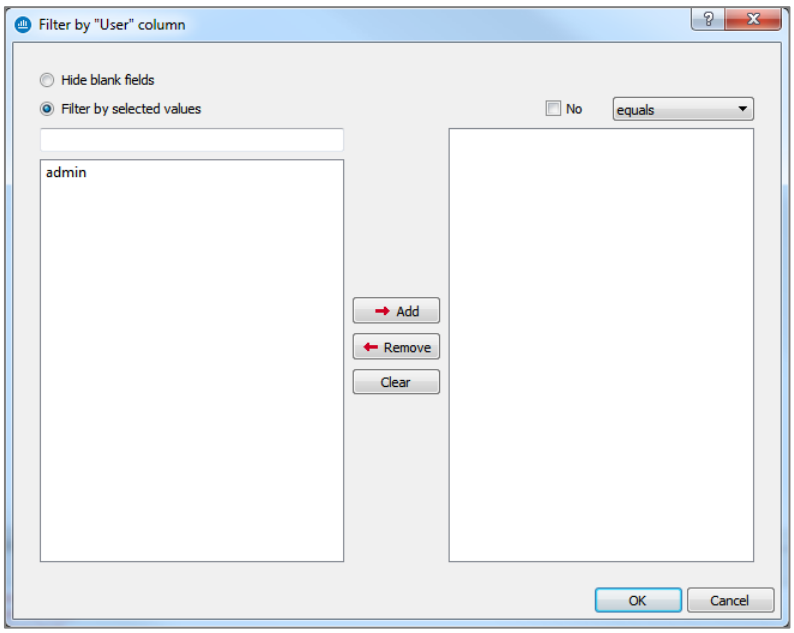


Figure 7: Filter by this column

The screen relates to the column that had been selected previously. *(E.g.: Filter by the "Details" column)*.

- **Hide blank fields** option: allows displaying only fields that contain data.
- **Filter by selected values**: a value can be entered manually or selected from the suggested list.

To create a filter, you only need to select one or several values from the suggested list and add them in order for them to appear in the section to the right of the table.

You may use the following operators:

- Equals: the values found have to be equal to those selected.
- Contains: looks for a word in a phrase
- Begins with: looks for a phrase beginning with a string
- Ends with: looks for a phrase ending with a string.
- Joker (Wildcard): *See the table below.*
- Regular expression: cf. http://qt-project.org/doc/qt-4.8/qregexp.html

c	E.g., if "c" is entered, the system will search for all occurrences of "c".
?	Allows searching for a single character.
*****	Allows searching for one or several characters.
[…]	Allows entering several characters between square brackets. For example, if [ABCD] is selected, the search will be conducted for A or B or C or D. If [A-D] is entered, the search will be for ABCD, if [A-Z] is entered, the search will be for all capital letters.

Events can therefore be filtered according to one or several values. For example, displaying events using the protocol HTTP or https.

It is also possible to negate a criterion by selecting the option **No**. For example, displaying all entries except if the protocol is HTTP.

- Columns can be resized according to their contents (option **Adjust columns to fit contents**).

Furthermore, the administrator can sort the table by clicking on the column by which he wishes to sort.

2.2.1.5.2 Contextual menu on lines

Right-clicking against a line will display a contextual menu that allows various operations. The options offered vary according to the table.

2.2.1.5.2.1 Overview

3 contextual menus can be opened in this window:

- When right-clicking against a firewall
- When right-clicking against an empty zone in the list of firewalls
- When right-clicking against in the "Connection logs" view

Contextual menu relating to a firewall

Show dashboard…	Opens the `Dashboard` menu of the selected firewall.
Generate an instant web report…	Clicking on this button will generate a report in HTML. This report will contain the following information at any given moment: system information, memory, connected users, services, Active Update status, bandwidth statistics, connection statistics, vulnerabilities, number of hosts, authenticated users, number of major and minor alarms, quarantine, the number of VPN tunnels, filter rules and configured IPSec tunnels.
This feature will run the web administration interface for firmware in version 9 or higher, otherwise Unified Manager will be launched	Allows logging on to the web administration interface of the selected firewall
Disconnect	Allows disconnecting from the selected firewall.
Remove this firewall from the connection list…	Enables disconnecting and deleting the entry that corresponds to this connection.
Add a new firewall to the connection list and connect to it	Displays the direct connection window to enable connecting to a firewall.
Add a firewall from the address book to the connection list	Opens the address book window to allow the selection of a registered firewall.
Add this firewall to the address book	Opens a window that will allow saving the selected firewall in the address book.
Edit the address book	Opens the address book window to enable editing.

Contextual menu from right-clicking against an empty zone	
Add a new firewall to the connection list and connect to it	Displays the direct connection window to enable connecting to a firewall.
Add a firewall from the address book to the connection list	Opens the address book window to allow the selection of a registered firewall.
Edit the address book	Opens the address book window to enable editing.

Contextual menu relating to connection logs	
Copy	Copies the selected log line(s).
Copy Link Location	Copies the location of the link.
Select all	Selects all the log lines.
Clear logs	Deletes all log lines.

2.2.1.5.2.2 Events

Right-clicking against a line containing an event will bring you to the contextual menu that will allow you to:

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
View source host…	Indicates the name of the source host. If this option is selected, the `Hosts` menu will open.
View destination host…	Indicates the name of the destination host.
Add the source host to the Object base	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall's object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".
Add the destination host to the Object base	This option allows: • Creating an object corresponding to the selected destination IP address directly in the firewall's object base in Stormshield Network Real Time Monitor • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".

Send source to quarantine	Allows quarantining the source host for a fixed period of 1 minute, 5 minutes, 30 minutes or 3 hours.
View packet...	Allows opening the tool that will allow viewing malicious packets.
Empty alarms	Purges the list of displayed alarms.
Copy to the clipboard	Copies the selected line to the clipboard.

2.2.1.5.2.3 Vulnerability Manager

In the Vulnerability tab, 3 contextual menus can be opened:

- When right-clicking against a line detailing a vulnerability
- When right-clicking against a line detailing a host
- When right-clicking against the help zone

Contextual menu relating to a vulnerability

Right-clicking against a line containing vulnerability will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

Contextual menu relating to a host

Right-clicking against a line containing a host will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by these criteria	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.

Add the host to the Object base	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall's object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".
View the host	The Hosts menu directory will open to display additional information on the detected host. During "pre-filtering", the host concerned will be selected. The data will be filtered according to the hostname if available, or by its address.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

In the Application tab, 2 contextual menus can be opened:

- When right-clicking against a line detailing an application
- When right-clicking against a line detailing a host

Contextual menu for a line containing an application

Right-clicking against a line containing an application will bring you to the contextual menu that will allow you to:

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE:** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard:	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu for a line containing a host

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". Caution: this is a new filter system… **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View the host	The Hosts menu directory will open to display additional information on the detected host. During "pre-filtering", the host concerned will be selected. The data will be filtered according to the hostname if available, or by its address.
Add the host to the Object base	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall's object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".

In the Information tab, 3 contextual menus can be opened:

- When right-clicking against a line containing information
- When right-clicking against a line detailing a host
- When right-clicking against the help zone

Contextual menu for a line containing information

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.

Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu for a line containing an event

Right-clicking against a line containing an event will bring you to the contextual menu that will allow you to:

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View the host	The Hosts menu directory will open to display additional information on the detected host. During "pre-filtering", the host concerned will be selected. The data will be filtered according to the hostname if available, or by its address.
Add the host to the Object base	This option allows: • Creating an object corresponding to the selected source IP address directly in the firewall's object base in Stormshield Network Real Time Monitor. • Adding this object to an existing group on the firewall. For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

2.2.1.5.2.4 Hosts

Many contextual menus can be opened in this window:

- When right-clicking against a host
- When right-clicking against the "Vulnerabilities" tab
- When right-clicking against the "Applications" tab
- When right-clicking against the "Information" tab
- When right-clicking against the "Connections" tab
- When right-clicking against the "Events" tab
- When right-clicking against the help zone

Contextual menu relating to a host

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Remove host from ASQ…	Enables deleting the host's ASQ information. This may be useful especially if a host has been hacked. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action.
Reset Vulnerability Manager information	Resets VULNERABILITY MANAGER data for the selected host. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action. When you perform this reset, the host will be deleted from the VULNERABILITY MANAGER database and as well as from data counters (detected vulnerabilities, software…).
Send to quarantine	The quarantined host will be dynamically blocked for a duration to be specified. (This duration can either be 1 minute, 5 minutes, 30 minutes or 3 hours). The "Monitor modify" privilege is necessary. You will not be asked to confirm this action.
Manually set the Operating System	This option allows specifying a host's operating system when Stormshield Network Vulnerability Manager is unable to detect it automatically. The window will then offer several fields: **Current operating system**: The OS that Stormshield Network VULNERABILITY MANAGER uses for detecting vulnerabilities on a host. The OS of a host may not be detected sometimes. **Detected operating system**: OS that Stormshield Network VULNERABILITY MANAGER detects after performing a traffic scan on a host. The Restore button allows removing the OS indicated by the user and reverting to the OS detected by VULNERABILITY MANAGER.

New OS name: In the event the host's OS is not detected by VULNERABILITY MANAGER, it is possible to impose it by selecting it from the suggested list. In this case, 2 situations may arise:

1. You are unable to specify the correct version (*examples: Android, Blackberry, etc*). In this case, the "Version" field will remain grayed out. Click on OK in order to force the OS to accept this value.
2. You are able to specify the version (*example: Linux*). In this case, the "Version" field will be modifiable and you will be able to enter a version number (*example: 2.6*). Next, click on Validate. If VULNERABILITY MANAGER detects the version, a name will appear (*example, Linux 2.6.14*). To finish, click on OK in order to confirm your selection.

Imposing the host's OS when it has not been detected will allow, in particular, viewing the vulnerabilities of services and products according to the system.

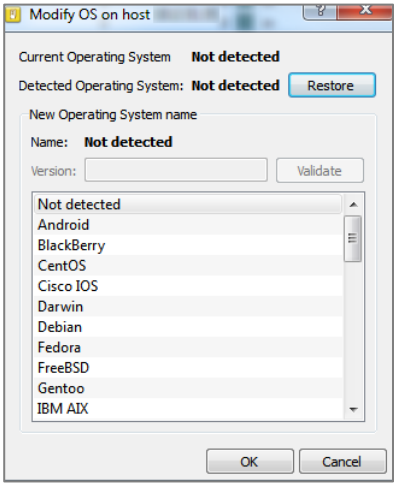


Figure 8: Manually set the OS

Add the host to the Object base

This option allows:

- Creating an object corresponding to the selected IP address directly in the firewall's object base in Stormshield Network Real Time Monitor.
- Adding this object to an existing group on the firewall.

For further information regarding this option, please refer to the Technical Note "Stormshield Network Collaborative Security".

Copy to the clipboard

Copies the selected line to the clipboard. Data can be copied in two different ways:

- A single line is selected: in this case, this line as well as the lines of details will be copied.
- Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu in the "Vulnerabilities" tab

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways:: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu in the "Applications" tab

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard. All the elements as well as the root element will be added to the clipboard.

Contextual menu in the "Informations" tab

Right-clicking against a line containing data will bring you to the contextual menu that will display the following information:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
List the hosts that present the same information	Allows filtering on hosts that have similar events.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu in the "Connections" tab

Right-clicking against a line containing a connection will bring you to the contextual menu that will display the following information:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View host	This option allows you to view only information of the selected host.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu in the "Events" tab

Right-clicking against a line containing an alarm will bring you to the contextual menu that will display the following information:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View the packet that raised the alarm	This will open the tool that will allow you to view malicious packets.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

2.2.1.5.2.5 Interfaces

Right-clicking against a line containing an interface will bring you to the contextual menu that will allow you to:

Filter by these criteria	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major".
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Display hosts associated with this interface	This option allows displaying the list of hosts that have the same interface.

2.2.1.5.2.6 Quality of Service

Please refer to chapter

QUALITY OF SERVICE (QoS)

2.2.1.5.2.7 Users

2 contextual menus can be opened in this window:

- When right-clicking against the "users" zone
- When right-clicking against an "administration sessions" zone

Contextual menu from right-clicking against the "users" zone

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Remove user from ASQ	Enables deleting the user's ASQ information. This may be useful especially if a user has been affected by an attack. The "Monitor modify" privilege is necessary. A message will appear, asking you to confirm this action.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

Contextual menu from right-clicking against the "administration sessions" zone

Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

2.2.1.5.2.8 Quarantine – ASQ Bypass

2 contextual menus can be opened in this window:

- When right-clicking against the "Quarantine" zone
- When right-clicking against an "ASQ Bypass" zone

Contextual menu from right-clicking against the "Quarantine" zone

Right-clicking against a line containing a quarantined host will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, when filtering by a particular firewall address, the administrator will obtain only all the relevant lines. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

Contextual menu from right-clicking against the "ASQ Bypass" zone

Right-clicking against a line containing a quarantined host will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, when filtering by a particular firewall address, the administrator will obtain only all the relevant lines. **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed a source address, the displayed list will only present the elements containing this source address.
Copy to the clipboard	Copies the selected line to the clipboard.

2.2.1.5.2.9 VPN Tunnels

This module now presents tunnels set up via IPSec VPN and SSL VPN under two separate tabs.

« SSL VPN Tunnels » tab

By right-clicking on a row of SSL VPN tunnels, you will access a contextual menu that allows you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field.

Filter only this column by this criterion	This option allows restricting the list of results to the criteria under your cursor. **Example** If your cursor pointed a username, the displayed list will only present the elements containing this username.
View host…	This option allows displaying in the Hosts module in Real Time Monitor all the characteristics of the host corresponding to the IP addresses (vulnerabilities, applications, connections, etc.).
Remove this tunnel	This option allows instantaneously shutting down the selected SSL VPN tunnel.

« IPSec VPN Tunnels» tab

Right-clicking against a line containing a VPN tunnel will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority “Major”, the administrator will get all the lines containing “Major”.
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
View logs of outgoing SPIs	This option will allow displaying the SPIs of the negotiated outgoing SA.
View logs of incoming SPIs	This option will allow displaying the SPIs of the negotiated incoming SA.
View the outgoing policy	Hypertext link enabling the display of the outgoing policy visible in the VPN Policy menu.
View the incoming policy	Hypertext link enabling the display of the incoming policy visible in the VPN Policy menu.
Reset this tunnel	The selected tunnel will be deleted, but the configuration on the firewalls will still be active. The SAs matching the selected tunnel will be cleared; new SAs will have to be renegotiated so that the tunnel can be used again.
Reset all tunnels	All tunnels will be deleted.

2.2.1.5.2.10 Active Update

Right-clicking against a line in the Active Update section will bring you to the contextual menu that will allow you to:

Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

2.2.1.5.2.11 Services

Right-clicking against a line containing a service will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the status "Enabled", the displayed list will only present the elements containing this status.
Copy to the clipboard	Copies the selected line to the clipboard. Data can be copied in two different ways: • A single line is selected: in this case, this line as well as the lines of details will be copied. • Several lines are selected: in this case, only these lines will be copied to the clipboard.

2.2.1.5.2.12 Hardware

This is the menu dedicated to high availability. Please refer to sections 3.2.7 and 5.4.

2.2.1.5.2.13 Filter policy

This menu allows you to view different types of rules :
Implicit rules

- Global filtering rules
- Local filtering rules
- NAT rules for local

For more information, please refer to section 6.1.

2.2.1.5.2.14 VPN Policy

Right-clicking against a line containing a VPN policy will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field.
View corresponding tunnels	This will open the VPN Tunnels menu with a filter.

2.2.1.5.2.15 Logs

VPN

Right-clicking against a line containing a VPN policy will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the priority "Major", the administrator will get all the lines containing "Major". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criteri	This option allows you to restrict the list of the results pointed to by the cursor. **Example** If your cursor pointed the destination / website consulted, the displayed list will only present the elements containing this destination / website.
Copy to the clipboard	Copies the selected line to the clipboard.

System

Right-clicking against a line in the System section will bring you to the contextual menu that will allow you to:

Filter this column by this criterion	This option allows restricting the list of results to the selected field. For example, if the data is filtered by the status "Enabled", the administrator will get all the lines containing "Enabled". **NOTE** Using this option will replace all the current filters on the columns
Filter only this column by this criterion	This option allows you to restrict the list of the results pointed to by the cursor.
Copy to the clipboard	Copies the selected line to the clipboard.

2.2.1.6 Status bar

Figure 9: Status bar

The status bar contains menus from the menu directory that may have been opened during a session. Being able to do so is particularly useful when you are monitoring several firewalls at a time. You will be able to get back the same information window for each firewall and thus make simultaneous comparisons.

2.2.1.7 Button bar

Figure 10: Button bar

This bar appears in most menus in Monitor.

2.2.1.7.1 Refresh

This button allows you to reinitialize the list displayed (Alarms, VULNERABILITY MANAGER, Hosts, Interfaces, Quality of Service, Users, Quarantine, VPN Tunnels, Active Update, Services, Hardware, Filter Policy, VPN, Logs).

2.2.1.7.2 Show/Hide help

This button allows you to show or hide a help screen. Subsequently, you only need to click on the selected line to get help when necessary.

2.2.1.7.3 Firewall

This drop-down menu allows you to filter the list of alarms on a selected firewall.

2.2.1.7.4 Duplicate

The window can be duplicated using the button found in it. This comes in handy especially when you wish to change the target (firewall or <all>) and view.

2.2.1.8 Search engine

The search zone is presented in 2 different formats:

1st format: the bar shown below can be seen on all screens except for the "Events" screen.

Figure 11: Search zone

2nd format: the bar below appears in the Events menu.

Figure 12: Search zone - Events

The **Filters** button contains the filters defined by the application and allows obtaining only the lines below:

- Alarm
- Virus
- Connection
- Web
- Mail
- FTP
- Filter
- SSL
- SSL VPN
- Authentication
- Applications (alarme)
- Protections (alarme)
- Malwares (alarme)

2.2.1.8.1 Search

In this zone, you will be able to conduct searches through elements in the list. Elements are filtered at the same time search criteria are being entered.

2.2.2 INTRODUCTION TO MENUS

2.2.2.1 File

The **File** menu concerns connections to the firewall and the application's general options.

Address book…	Configures the firewalls' address books.
Direct connection…	Opens a new Firewall connection window. Enter the IP address of the Firewall and the user password.
Application settings…	Determines the behavior that Monitor should adopt at startup, enables getting a packet analyzer, defining a destination folder for reports, and the language used in the graphical interface.
Default monitoring settings…	Configures memory, connection timeout and the frequency with which different parameters will be refreshed.
Quit	Disconnects monitors and shuts down the application.

2.2.2.2 Windows

The **Windows** menu enables managing the display windows of the different connected firewalls:

Maximize	Opens the selected window.
Cascade	Arranges the various connection windows in cascade.
Title	Gives a global view of the main services offered by Monitor.
Duplicate current window	Duplicates the current window according to the firewall that you had selected earlier.
Overview	IP address of connected firewall(s).
Firewall address	The drop-down menu indicates the last screens visited and identifies the current screen with a tick.

2.2.2.3 Applications

The **Applications** menu enables connecting to other applications in the Stormshield Network Administration Suite. Using the two shortcuts provided the added advantage of not having to reauthenticate on both applications.

Run the configuration application	Allows accessing the selected firewall's web administration interface.
Launch Stormshield EVENT REPORTER	Enables opening the Stormshield Network EVENT REPORTER module from the Administration Suite.

2.2.2.4 ? (Help)

Help	Opens a page that accesses your secure-access area, to allow you to obtain documentation.
About…	Provides information on the monitor in use (version number, credits).

2.2.3 APPLICATION SETTINGS

Certain parameters can be configured in the **REAL-TIME MONITOR** application.

- Select the menu **`File\Application settings…`**: the parameters window will appear.

2.2.3.1 Behavior at startup

This tab offers the different options that enable configuring the application's behavior at startup.

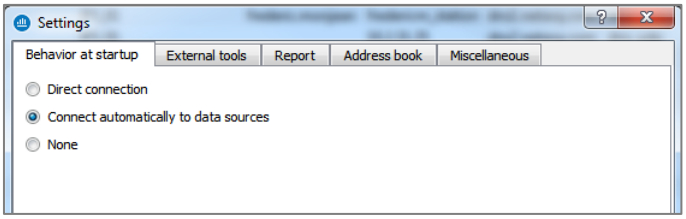


Figure 13: Behavior at startup

Direct connection	If this option is selected, the direct connection window will open when Monitor starts up. It will enable you to enter the IP address of the desired firewall and the user password.
Connect automatically to data sources	If this option is selected, the connection will be established automatically on different firewalls in the address book.
None	The `Overview` window will open but Monitor will not connect to any firewall.

2.2.3.2 External tools

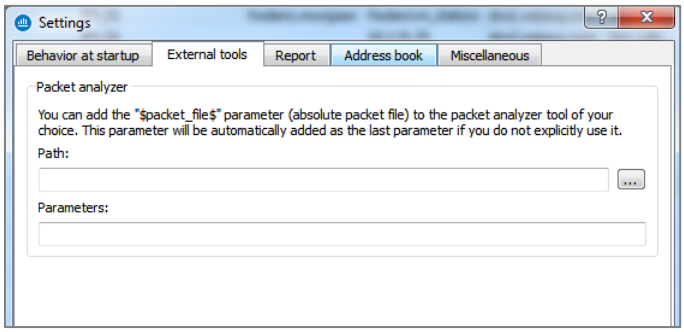


Figure 14: Settings – External tools

Packet analyzer	When an alarm is triggered on a Stormshield Network Firewall, the packet responsible for setting off the alarm can be viewed. In order to do this, you need a packet viewing tool like Ethereal or Packetyzer. Specify the selected tool in the field "Packet analyzer", which the Monitor will use to display malicious packets.
Path	Indicates the location of the directory containing the application that allows analyzing packets.
Parameters	The parameter "$packet_file$" can be added to the packet analyzer.

2.2.3.3 Report

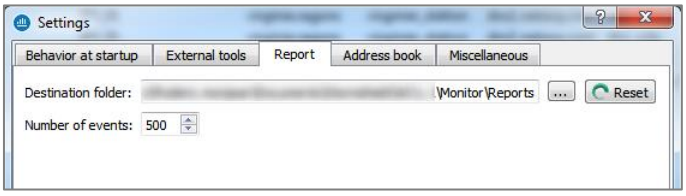


Figure 15: Settings – Report

Destination folder	Enables selecting the destination folder for the report. The **Reset** button allows you to reset the directory for storing reports.
Number of events	Allows defining the number of events desired when generating the report. By default, the value is set to 500 lines.

REMARK

The report can be generated by right-clicking on a line in the **Overview** menu and by selecting the option **Generate a web report...**

The report contains the following information:

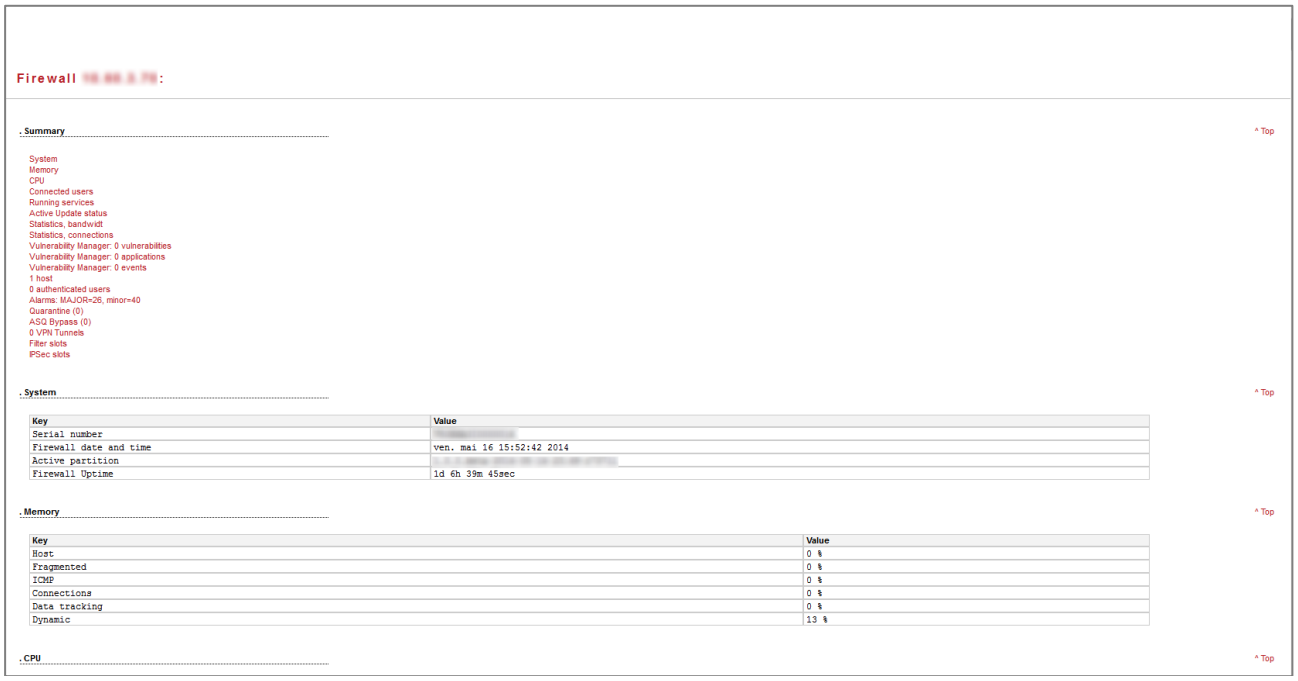


Figure 16: Synthesis report

It displays information regarding the firewall for which you intended to generate a report. By clicking on a link in the list, the information will be displayed in table or graph form.

In the example below, information on memory is displayed.

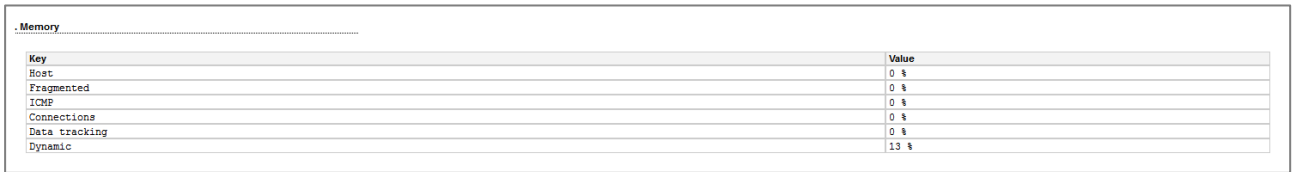


Figure 17: Memory information

2.2.3.4 Address book

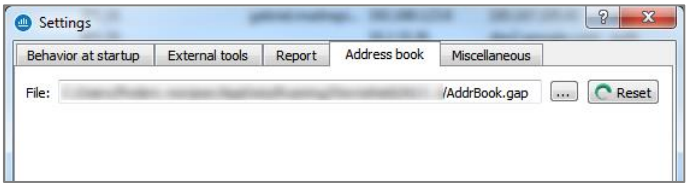


Figure 18: Settings – Address book

The Stormshield Network UNIFIED MANAGER, Stormshield NetworkREAL-TIME MONITOR and Stormshield NetworkEVENT REPORTER applications use the same address book and therefore the same address book file.

To retrieve a .gap file (Stormshield Network project file), simply click on “Browse”.

2.2.3.5 Miscellaneous

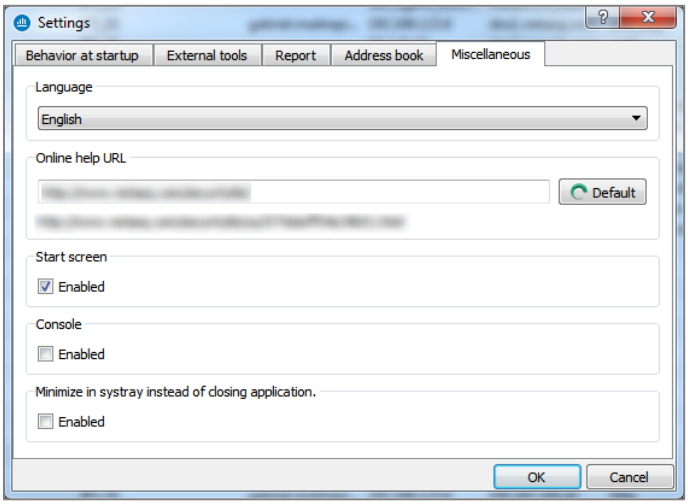


Figure 19: Settings – Miscellaneous

Language	You can select a language for the interface's menus. The automatic selection will choose the language installed on the PC's Windows OS. After a language selection, the Firewall Monitor must be restarted in order to apply the change.
Online help URL	This option allows you to access at any time at the knowledge base.
Splash screen	If you select this option, the first window that appears on startup will contain the name, logo, version and loading status of the software. If it is not selected, the start screen will no longer be displayed.
Console	If the option Enable is selected, you will be able to access firewalls in console mode (CLI commands). When this window is validated, a `Console` menu will be added under the `Overview` menu directory.
Minimize in systray instead of closing application	If this option is selected, the application will be minimized in Systray instead of being shut down.

2.2.4 DEFAULT MONITORING SETTINGS

This menu enables configuring when all information contained in Monitor will be refreshed. There are 6 parameters that regulate the frequence of data retrieval. You can define how long the different logs (in number of lines) and datagrams (in minutes) will be displayed.

➲ The default parameters for monitoring can be accessed from the menu **File\Default monitoring settings.**

2.2.4.1 Updates

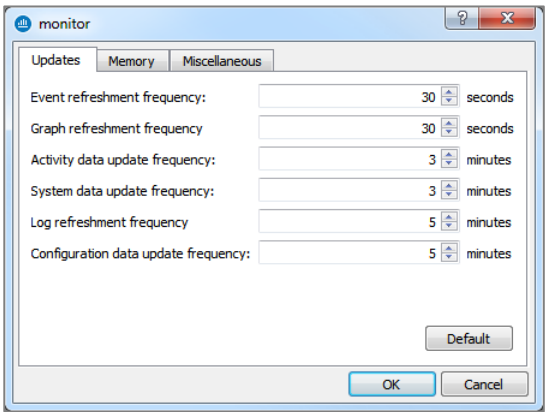


Figure 20: Monitor – Updates

Event refreshment frequency	Specifies in seconds when the list of detected events will be refreshed. The refreshment frequency is set to 30 seconds by default and may be a minimum of 1 second and a maximum of 3600 seconds.
Graph refreshment frequency	Specifies in seconds when graphs (Statistics, Interfaces, QoS and VPN SA) will be refreshed. The refreshment frequency is set to 30 seconds by default and may be a minimum of 10 seconds.
Activity data refreshment frequency	Specifies in minutes when activity data (hosts, authenticated users and Vulnerability Manager) will be refreshed. The refreshment frequency is set to 3 minutes by default and may be a minimum of 1 minute.
System data refreshment frequency	Specifies in minutes when system data (session data, high availability, RAID, cryptography card, quarantine, services and Active Update) will be refreshed. The refreshment frequency is set to 3 minutes by default and may be a minimum of 1 minute.
Log refreshment frequency	Specifies in minutes when log data (Log space, filters, VPN, system, traffic and filter logs) will be refreshed. The refreshment frequency is set to 5 minutes by default and may be a minimum of 1 minute.
Configuration data update frequency	Specifies in minutes when configuration data (Anti spam, anti-virus, proxies, SPD and system properties) will be refreshed. The refreshment frequency is set to 5 minutes by default and may be a minimum of 1 minute.

REMARK

The Default button allows you to reset the parameters to their default values.

2.2.4.2 Memory

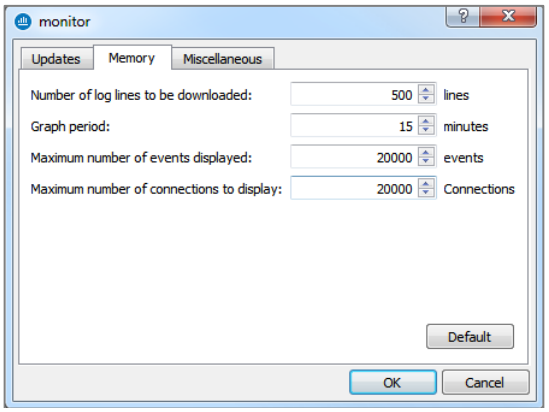


Figure 21: Monitor – Memory

Number of log lines to be downloaded	Configures the number of log lines you wish to display in the `Traffic` menu.
Graph period	Indicates how long graphs will be displayed (Statistics from the `Interfaces` menu).
Maximum number of events displayed	Configures the number of event lines that you wish to display in the `Events` menu. By default, the value is set to 20,000 events and may be a minimum of 1 events and a maximum of 2,000,000 events. The number of alarm lines indicated influences the memory used: The memory used for 150,000 event lines indicated for a firewall is about 220 MB. The memory used for 300,000 event lines indicated for a firewall is about 430 MB.
Maximum number of connections displayed	Configures the maximum number of connections that you wish to display in the Hosts, Interfaces, Filter policy and Quality of Service modules. If the value is zero, the function will be disabled. By default, the value is set to 20,000 events.

2.2.4.3 Miscellaneous

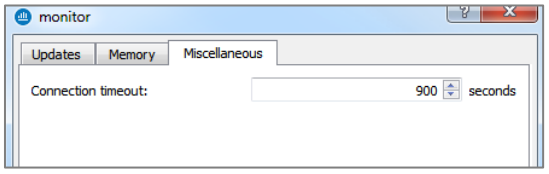


Figure 22: Monitor – Miscellaneous

Connection timeout	When the firewall does not respond, the connection will be shut down at the end of the period determined in this field.

3 INFORMATION ON FIREWALLS

3.1 OVERVIEW

3.1.1 Introduction

From the menu directory, the **Overview** menu allows you to display several types of information regarding your firewalls. Once the connection with the firewall is established, this information will be available.

The **Overview** menu consists of five zones:

- The menu directory
- An overview of information on vulnerabilities found on your network (Corresponds to the *Part 4/Chapter2: VULNERABILITY MANAGER* menu).
- A search and icon bar
- A list of your firewalls
- A view of connection logs

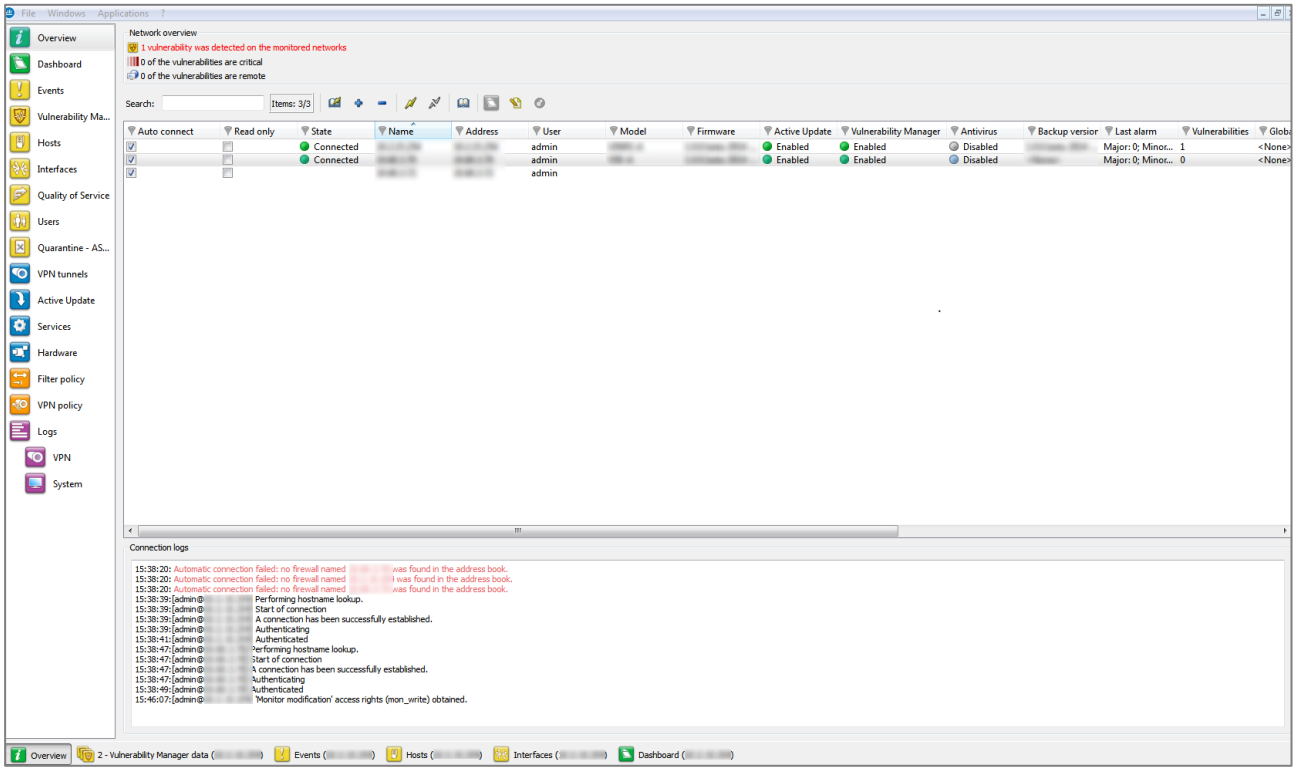


Figure 23: Overview

3.1.2 Overview of information on vulnerabilities

This view indicates the number of vulnerabilities found, the number of critical vulnerabilities and the number of vulnerabilities that are remotely accessible on your networks. These indications represent links that allowing access to these vulnerabilities (VULNERABILITY MANAGER menu).

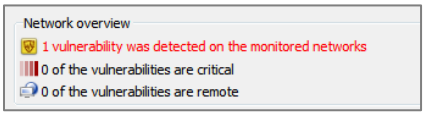


Figure 24: Network overview

3.1.3 List of firewalls

This view provides the following information on your product(s):

Auto connect	Selecting this option allows you to activate automatic reconnection of **REAL-TIME MONITOR** in the event of a disconnection.
Read-only	Select this option to activate read-only mode.
State	Indicates the product's connection status. Options: **Connected/Disconnected**.
Name	Product's name or IP address if the name has not been indicated.
Address	Firewall's IP address.
User	Login of the connected administrator account.
Model	Product model: SN200, SN6000…
Firmware	Version of the firmware monitored in Firewall Monitor's "Firmware".
Active Update	Indicates the update status of the Active Update module. Options: **OK** or **x failure (s)**.
VULNERABILITY MANAGER	Indicates the number of vulnerabilities.
Antivirus	Indicates the status of the antivirus. Options: **OK/Disabled**.
Backup version	Version number of the backup module or of the firmware in the passive partition.
Last alarms	Indicates the number of major and minor alarms for the latest alarms (over the past 15 minutes). The maximum value is 100 even if the number of alarms exceeds this value.
Vulnerabilities	Indicates the number of vulnerabilities.
Global filter	Indicates whether a global filter rule has been activated. If so, "Global policy" will be indicated.
Filter	Indicates the name of the active filter slot.
VPN	Indicates the name of the active VPN slot.
URL	Indicates the name of the active URL slot.
NAT	Indicates the name of the active NAT slot.
Uptime	Amount of time that the firewall has been running since the last startup.
Session	Indicates the number of sessions opened on the firewall.
Comments	Comments or descriptions of the firewall.

3.1.4 Connection logs

This window indicates logs of connections between **REAL-TIME MONITOR** and the firewall.

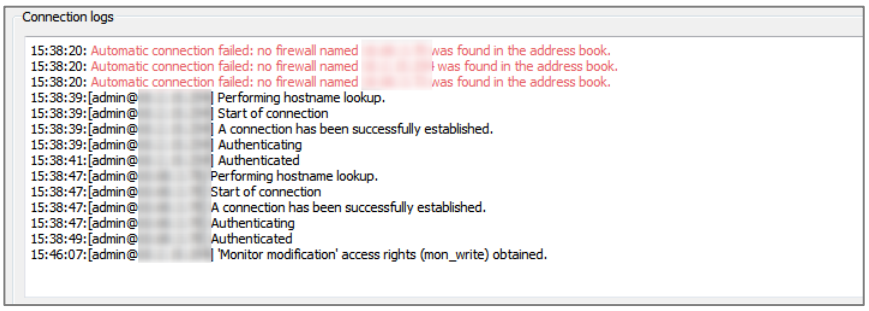


Figure 25: Connection logs

TIP

You can erase logs by right-clicking on the "Connection logs" view DASHBOARD

3.2 DASHBOARD

3.2.1 Introduction

The **Dashboard** menu allows displaying on a single screen all the useful information concerning real-time monitoring.

It basically picks out useful information from some of the menus in the **Stormshield Network REAL-TIME MONITOR** menu directory and adds on other additional information. The data displayed in this window are:

- System information
- Memory
- CPU
- Hardware
- Active network policies
- Alarms
- Vulnerabilities
- VPN tunnels
- Active Update
- Logs
- Services
- HTTP Cache
- Interfaces
- Top 5 interfaces for incoming throughput
- Top 5 interfaces for outgoing throughput
- Top 5 hosts for incoming throughput
- Top 5 hosts for outgoing throughput

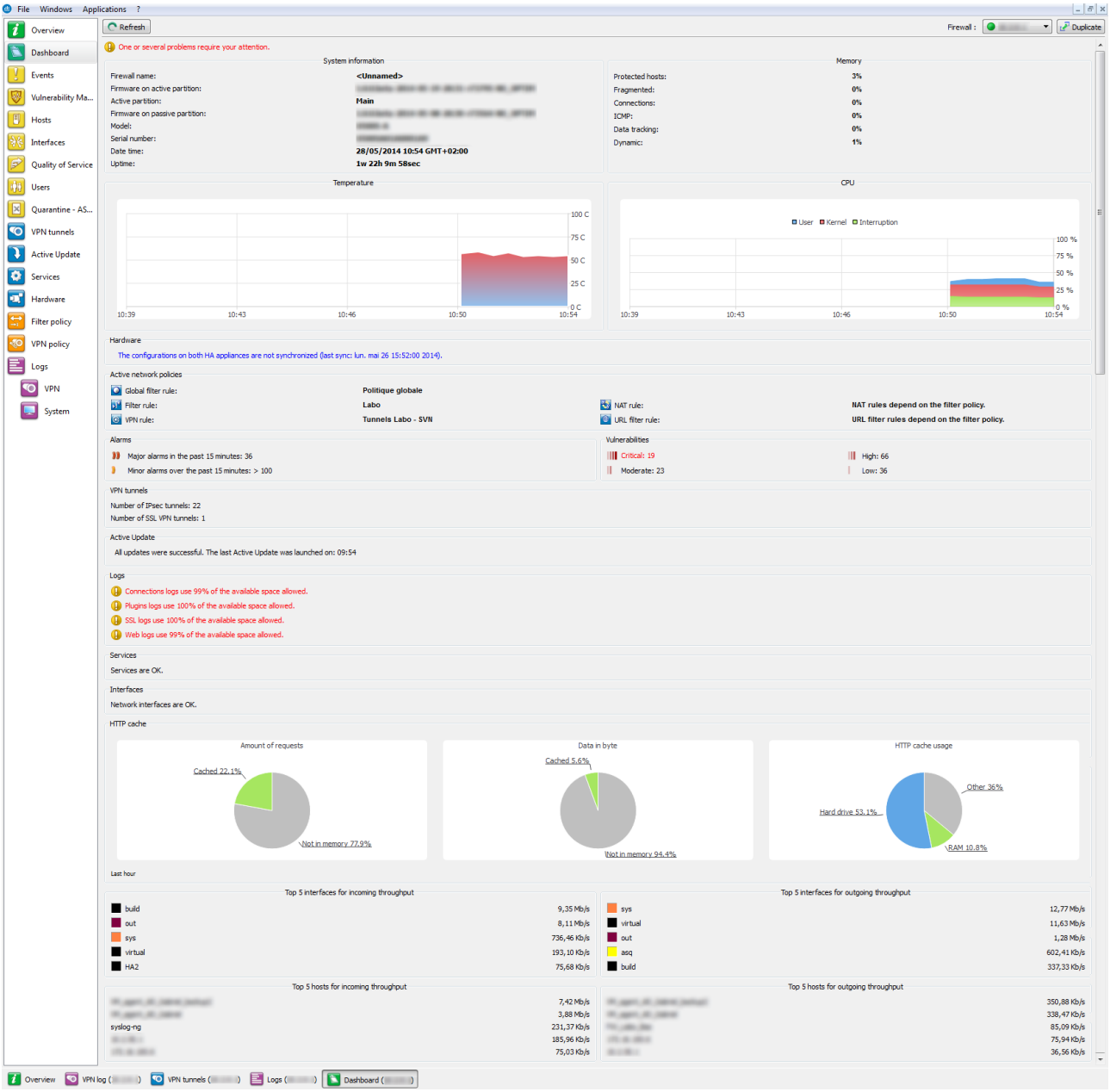


Figure 26: Dashboard

3.2.2 Selecting a product

When you click on the **Dashboard** menu, a product selector window may open if several firewalls have been registered.

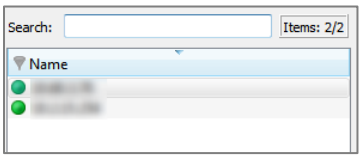


Figure 27: Search

1. If the list of firewalls is long, look for the desired firewall using the **Search** field.
2. Select the firewall.
3. Click on **OK**. The Dashboard of the desired firewall will appear.

3.2.3 System information

Firewall name	Name given to the product when it was registered in the address book.
Firmware on active partition	Version of the active partition's firmware.
Active Partition	Partition on which the firewall was booted.
Firmware on passive partition	Version of the passive partition's firmware.
Model	Firewall's model number.
Serial number	Firewall's serial number.
Date-time	Current date and time.
Uptime	Amount of time that the firewall has been running since the last startup.

3.2.4 Memory

This refers to the use (in percentage) of memory reserved for storing information (buffer). The buffer is linked to the *stateful* module and corresponds to saving the context.

Protected host	Protected host stack
Fragmented	Fragmented packets
Connections	All TCP/IP connections.
ICMP	ICMP requests (Ping, trace route...).
Data tracking	Memory used for monitoring connections.
Dynamic	Percentage of ASQ memory being used.

Buffer sizes vary according to product type and product version.

Cleaning algorithms optimize the operation of "Hosts", "Fragmented", "ICMP" and "Connections" buffers. Entries in the "Fragmented" and "ICMP" buffers are initialized at fixed intervals (each entry has a limited lifetime: TTL).

This illustrates part of the Firewall's activity. A high percentage may mean the Firewall is overloaded or that an attack has been launched.

3.2.5 CPU

DEFINITION

Better known as a “processor”, this is the internal firewall resource that performs the necessary calculations.

User:	CPU time allocated to the management of user processes.
Kernel:	CPU time that the kernel consumes
Interruption:	CPU time allocated for interruptions.

3.2.6 Temperature

This graph displays the temperature of the appliance in degrees Celsius (°C). This temperature is not available on virtual machines. For multi-core processors, the value displayed is the average of all the CPUs.

3.2.7 Hardware

DEFINITION OF “HIGH AVAILABILITY”

A specific architecture in which a backup firewall takes over when the “main” firewall breaks down while in use. This switch is totally transparent to the user.

If high availability has been activated, an additional section will provide you with the information regarding high availability (status of firewalls, licenses, synchronization).

Click on the descriptive phrase in the “Hardware” zone in order to display the **Hardware** menu and to obtain information on high availability and the status of the firewall’s components (S.M.A.R.T. peripherals, RAID volumes where possible, disks and power supply units).

If the backup firewall is not available, information on the active firewall can be viewed.

Figure 28: Hardware

3.2.8 Active network policies

This view indicates whether slots are active. If so, the label of the activated rule is indicated. The rules mentioned here are:

Global filter rule	Name of the activated global filter policy.
Filter rule:	Name of the activated filter policy.
VPN rule	Name of the activated VPN rule.
NAT rule	Name of the activated translation policy.
URL filter rule	Name of the activated URL filter rule.

REMARK

<None> means that no policy has been activated for the rule that contains this indication.

3.2.9 Alarms

This view indicates the number of major and minor alarms during the past 15 minutes that the product has been connected. The maximum value indicated is 100 even if the number of alarms exceeds this value.

To view the alarms, click on either link of your choice – the **Events** menu will appear and will set out the list of alarms according to the selected criticality.

3.2.10 Vulnerabilities

This view indicates the number of vulnerabilities for a specific level. The 4 levels of vulnerability are: Critical, High, Moderate, Low.

To view a list of vulnerabilities, click on one of the levels, and the menu **Vulnerability management** will appear (*Cf.* chapter Vulnerability Manager).

3.2.11 VPN Tunnels

This view indicates the number of configured VPN tunnels. To view a list of configured VPN tunnels, click on the link – the **VPN Tunnels** menu will appear.

3.2.12 Active Update

This view indicates the status of updates that have been performed (success or failure) as well as the last time the "Active Update" module had been launched (date and time). To view a list of updates and their status, click on the link – the **Active Update** menu will appear.

3.2.13 Logs

This window indicates whether there are problems with the logs. To view a graph that represents the current size of the log file in real time (Alarms, Authentication, Connections, Filters, Monitor, Plugins, POP3, VULNERABILITY MANAGER, Administration, SMTP, System, IPSec VPN, Web, SSL VPN) in relation to the space allocated to each log type on the firewall, click on the link. The **Logs** menu will appear.

3.2.14 Services

This zone indicates whether there are problems with the services. To view a list of services and their status (**Enabled/Disabled**), click on the link – the **Services** menu will appear.

3.2.15 Proxy Cache

These 3 pie charts represent the use of the http cache when it has been enabled in the filter rules:

- The first graph compares the number of cached requests and the number of requests that were not saved in memory.
- The second graph compares the amount of cached data and the amount of data not saved in memory.
- The third graph represents the distribution of cached data on the hard disk, data cached in RAM and data not saved in memory.

3.2.16 Interfaces

This zone indicates whether there are problems with the interfaces. To view information on bandwidth, connections and throughput, click on the link. The **Interfaces** menu will appear.

3.2.17 Top 5 interfaces for incoming throughput

This zone displays the list of the 5 interfaces that have registered the most incoming throughput. Click on any one of the interfaces to display the Throughput tab graph in the **Interfaces** menu.

3.2.18 Top 5 interfaces for outgoing throughput

This zone displays the list of the 5 interfaces that have registered the most incoming throughput. Click on any one of the interfaces to display the Throughput tab graph in the **Interfaces** menu.

3.2.19 Top 5 hosts for incoming throughput

This zone displays the list of the 5 hosts that have registered the most incoming throughput. Click on any one of the interfaces to display the throughput tab graph in the **Interfaces** menu.

3.2.20 Top 5 hosts for outgoing throughput

This zone displays the list of the 5 hosts that have registered the most outgoing throughput. Click on any one of the interfaces to display the throughput tab graph in the **Interfaces** menu.

4 REAL-TIME INFORMATION

4.1 EVENTS

The alarms generated by the Firewall will appear in this window.

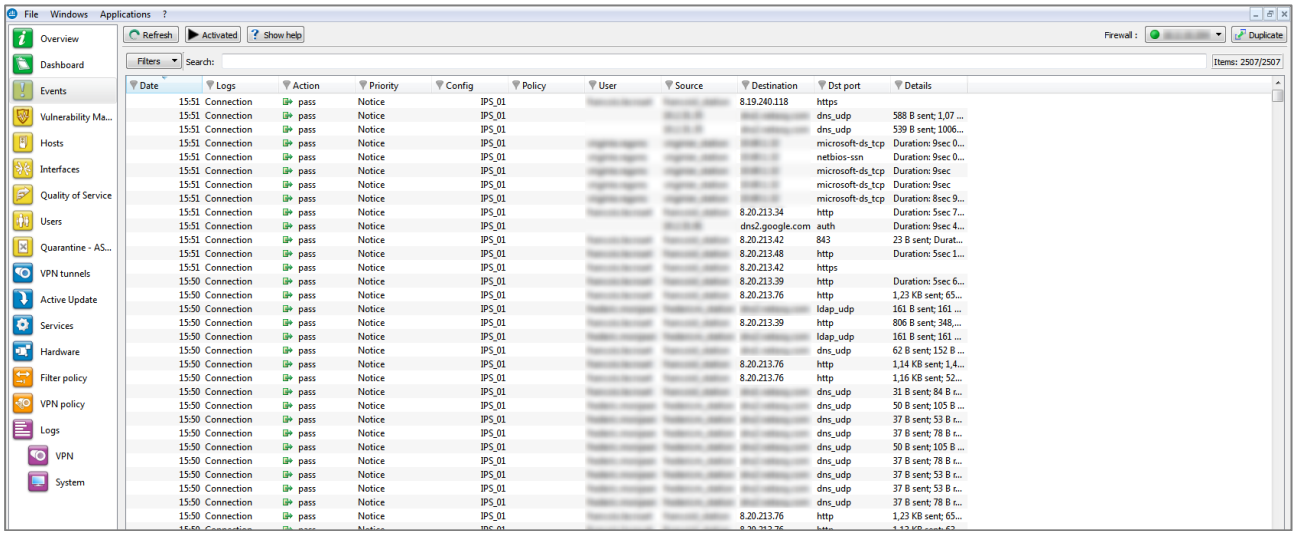


Figure 29: Events

In this module, the additional **Active/Suspended** button allows switching the status of alarm refreshment. If this button is in a suspended status, the automatic refreshment will be disabled, making it easier to read logs.

When the **Events** menu in the menu directory is selected, the data displayed by default are:

Date (time)	Date and time the line was recorded in the log file at the firewall's local time.
Logs	Indicates the type of logs (the possible types of logs are: Alarm, Plugin, Connection, Web, SMTP, FTP, POP3, Filter).
Action (action)	Action associated with the filter rule and applied on the packet (**Examples**: Block/Pass…)
Priority (pri)	Determines the alarm level. The possible values are: 0: emergency 1: alert 2: critical 3: error 4: warning 5: notice 6: information 7: debug
Config	Name of the application inspection profile that reported the event.
Policy	Name of the SMTP, URL or SSL filter policy that raised the alarm
User	Identifier for the authenticated user (ftp), e-mail address of the sender (SMTP), identifier for the user if authentication has been enabled (WEB).
Source	IP address or name of the object corresponding to the source host of the packet that

	set off the alarm.
Src prt num	Source port number involved, displayed in digital.
Destination	IP address or name of the object corresponding to the destination host of the packet that set off the alarm.
Dst port	Destination port number of the service or name of the object corresponding to the service port of the destination host if it exists and is requested for this connection.
Details	Description of the event relating to the log. This column groups some of the information gathered from the other columns. **Example** If an alarm log is concerned, information such as whether it was a sensitive alarm, the number of the filter rule, rule ID (already given in the columns "Sensitive alarm", "Rule" and "Rule ID") will be grouped in this column. This column displays the icon that specifies the type of detection according to the categories ***Applications***, ***Malware*** and ***Protections***.

Other available data are:

Firewall (fw)	Serial number or name of the firewall (if known) that caused the event.
UTC Date (time+tz)	UTC date (replaces the GMT)
Start date (starttime)	"Local" date at the start of an event.
UTC start date (startime+tz)	UTC date at the start of an event (a connection).
Timezone (tz)	Firewall's timezone.
Rule (ruleid)	Number of the filter rule involved in the raised alarm.
Protocol (proto)	Protocol of the packet that set off the alarm.
Connection group (groupid)	Identifier that would allow tracking child connections.
Source interface (srcif/srcifname)	Name of the firewall interface on which the event was raised (source interface network card).
Source address (src)	IP address of the source host of the packet that set off the event.
Source port (srcport/srcportname)	Source port number of the service or the name of the object corresponding to the service port of the source host (only if TCP/UDP).
Destination interface (dstif/dstifname)	Network card of the destination interface.
Destination address (dst)	IP address of the destination host of the packet that set off the event.
Authentication	Authentication method used.
Sensitive alarm (sensitive)	Indicates whether an alarm is sensitive. This alarm is raised whenever the intrusion prevention system detects a sensitive packet and for which it has been configured in intrusion detection mode. If the alarm is sensitive, an icon in the form of an exclamation mark followed by "Yes" will appear. Otherwise, "No" will be indicated. When the alarm is blocked, the icon will be grayed out (it is disabled). **NOTE** Only protocol alarms can be described as "sensitive". For alarms that are not in this class, the column will be empty.

Copy (repeat)	Indicates the number of an event's occurrences within a defined period. This period is configured in Stormshield Network UNIFIED MANAGER in the menu "`Logs\Advanced`", option **Write log duplicates every**.
Identifier (Id/alarmid)	Indicates the number of the alarm.
Context (class)	Text indicating the category to which the alarm belongs (system, protocol, filter, etc).
Alarm type (classification)	Code (number) indicating the alarm category. This column also displays the type of detection according to the categories **Applications, Malware** and **Protections**.
Caller	VoIP: Indicates the caller
Callee	VoIP: Indicates the callee
Duration	Connection time in seconds.
Sent	Number of KB sent during the connection.
Received (rcvd)	Number of KB received during the connection.
Operation (op)	Identified command of the protocol. • FTP: PUT, MPUT, GET, DELETE,… • HTTP: GET, PUT, POST,… • EDONKEY: SENDPART • POP3: RETR, LIST,… • FTP: DELETE, LIST,…
Result	Result of the operation in the protocol (example: 404 which indicates an error).
Parameter (arg)	Operation parameter.
Category (cat_site)	Web category of the requested website.
Spam level (spamlevel)	Spam level: 0 (Message not spam) 1,2 and 3 (spam) x (error during the treatment of the message) and ? (the nature of the message could not be determined) if antispam has been enabled.
Virus (virus)	Indicates whether there is a virus (if the antivirus has been enabled).
IP (ipproto)	Internet protocol (tcp or udp).
Media)	Type of traffic detected (audio, video, application,…)
Message (Msg)	Detailed description of the alarm. All commands sent by the client are found here. Sensitive information such as passwords is removed.
ICMP code (icmpcode)	ICMP code in the alarm logs.
ICMP type (icmptype)	ICMP type in the alarm logs.
Packet	Indicates the IP packet for which the alarm was raised. Right-clicking on this packet allows it to be viewed through a packet analyzer. The information displayed in this column shows the size of the IPv4 packets (value beginning with 45). The size of captured packets is 1536 bytes. **WARNING** To view a packet, a software program needs to be installed on your workstation.

NOTE

The logs will now be displayed for models without hard drive.

4.2 SN Vulnerability Manager (NVM)

4.2.1 Introduction

Stormshield Network VULNERABILITY MANAGER is a module that allows network administrators to gather information in real time and to analyze it in order to spot possible vulnerabilities that may compromise the security of their networks. Among other things, it also allows raising alarms generated by ASQ and thus to maintain an optimal security policy.

Stormshield Network VULNERABILITY MANAGER collects and archives in particular, information relating to the operating system, to various active services as well as to the different applications that have been installed. As a result, descriptive profiles can be made of network elements.

The following are **Stormshield Network VULNERABILITY MANAGER**'s aims:

- To configure your company network's security policy
- To analyze the status of the risk
- To optimize the level of security
- To report security events

The procedure is as follows:

1. Stormshield Network's intrusion prevention engine (ASQ) extracts data in real time using network protocols that it knows.
2. VULNERABILITY MANAGER then combines and weights these data.
3. The vulnerability found can then be treated using databases that have been indexed dynamically. Once all this information has been collected, they will be used in Monitor so that flaws on the network can be corrected, or prohibited software can be detected, or the real risk relating to the attack can be identified in real time.
4. The profile is therefore complete.
5. One or several solutions can thus be considered.

> **Example**
>
> A company has a public website that it updates twice a month via FTP. At a specific date and time, a vulnerability that affects FTP servers is raised and Monitor immediately takes it into account, enabling the network administrator to detect it at practically the same time.
> This vulnerability is represented by a line that indicates the number of affected hosts and whether a solution is available.
> By deploying this line, details of the hosts concerned will appear, as well as the service that has been affected by the vulnerability. Help, in the form of links, may be suggested to correct the detected flaw.

Once the network administrator becomes aware of the vulnerability, he can correct it at any moment, quarantine the affected host(s) and generate a report.

VULNERABILITY MANAGER can also perform weekly, monthly or yearly analyses, using the application **Stormshield Network EVENT REPORTER** (Autoreport). (*See the* **Stormshield Network EVENT REPORTER** *user guide.*)

When you click on the VULNERABILITY MANAGER menu in the menu directory, the scan window will consist of the following

- A Vulnerabilities tab
- An Applications tab
- An Events tab

4.2.2 Vulnerabilities tab

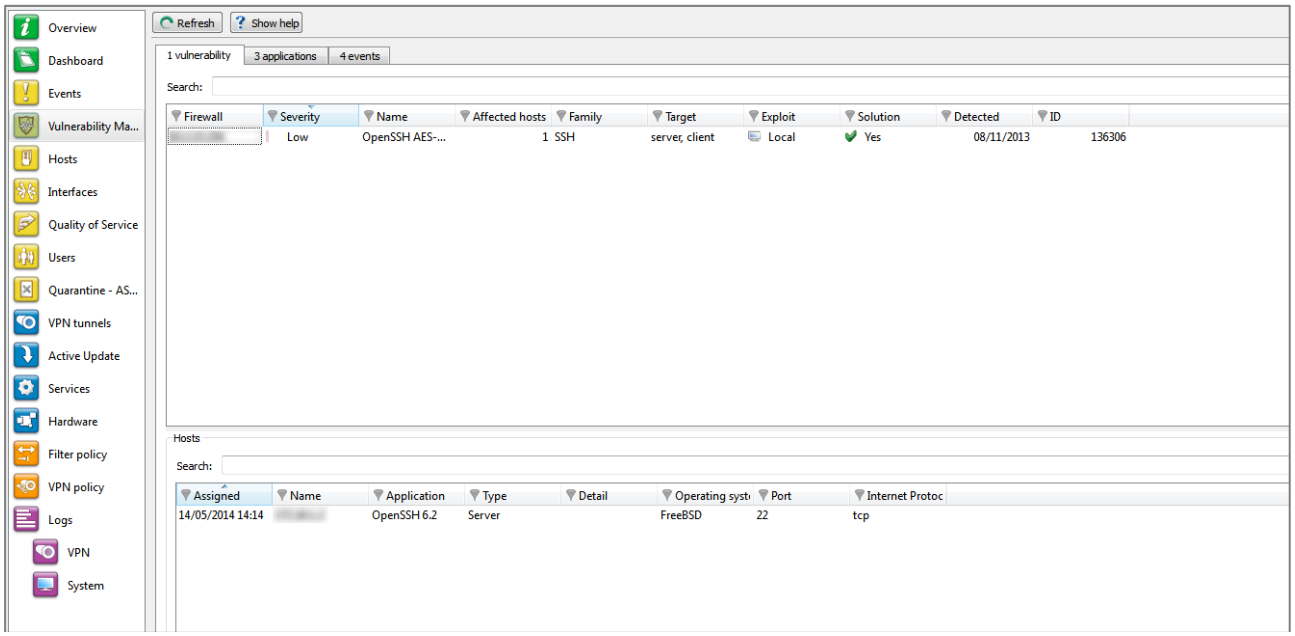


Figure 30: VULNERABILITY MANAGER

The window has 3 views:

- A view of the list of vulnerabilities
- A view of the list of hosts affected by this vulnerability
- A view allowing the resolution of the selected vulnerability if a solution exists

4.2.2.1 "Vulnerability(ies)" view

This view allows you to view all the vulnerabilities that the firewall has detected. Each line represents a vulnerability.

REMARK

The number of vulnerabilities is displayed in the tab's label.

The information provided in the "vulnerability" view is as follows:

Firewall	Serial number or name (if known) of the firewall at the source of the vulnerability.
Severity	Indicates the how severely the host(s) have/has been affected by the vulnerability, according to 4 levels: **Low**, **Moderate**, **High**, **Critical**.
Name	Indicates the name of the vulnerability.
Affected hosts	Number of hosts affected by the vulnerability.
Family	Family to which the vulnerability belongs.
Target	One of 2 targets: **Client** or **Server**.
Exploit	Local or remote access (via the network). Allows exploiting the vulnerability.
Solution	Indicates whether a solution has been suggested.
Release	Date on which the vulnerability was discovered. **WARNING** This refers to the date on which the vulnerability was discovered and not the date on which it appeared on the network.
ID	Allows a unique identification of the vulnerability.

4.2.2.2 "Hosts" view

This view allows you to view all the vulnerabilities for a given host. Each line represents a host.

The information provided in the "Hosts" view is as follows:

Affected	Date on which the host was affected.
Name	Name of the host affected by the attack (if it exists).
Address	IP address of the host affected by the attack.
Application	Name and version of the application (if available).
Type	Application type (Client/Server/Operating system).
Detail	Name of the service prone to being affected by the vulnerability.
Operating system	OS used.
Port	Number of the port on which the vulnerability had been detected.
Protocol	Name of the protocol used.

4.2.2.3 Help zone

The help zone allows you to get more details relating to the attack. Thus the administrator can correct the vulnerability.

Click on the **Show help** button to show or hide the help zone associated with a vulnerability.

Typically, help comes in the form of a descriptive file that contains explanations, links to the publisher's site or to bug fixes.

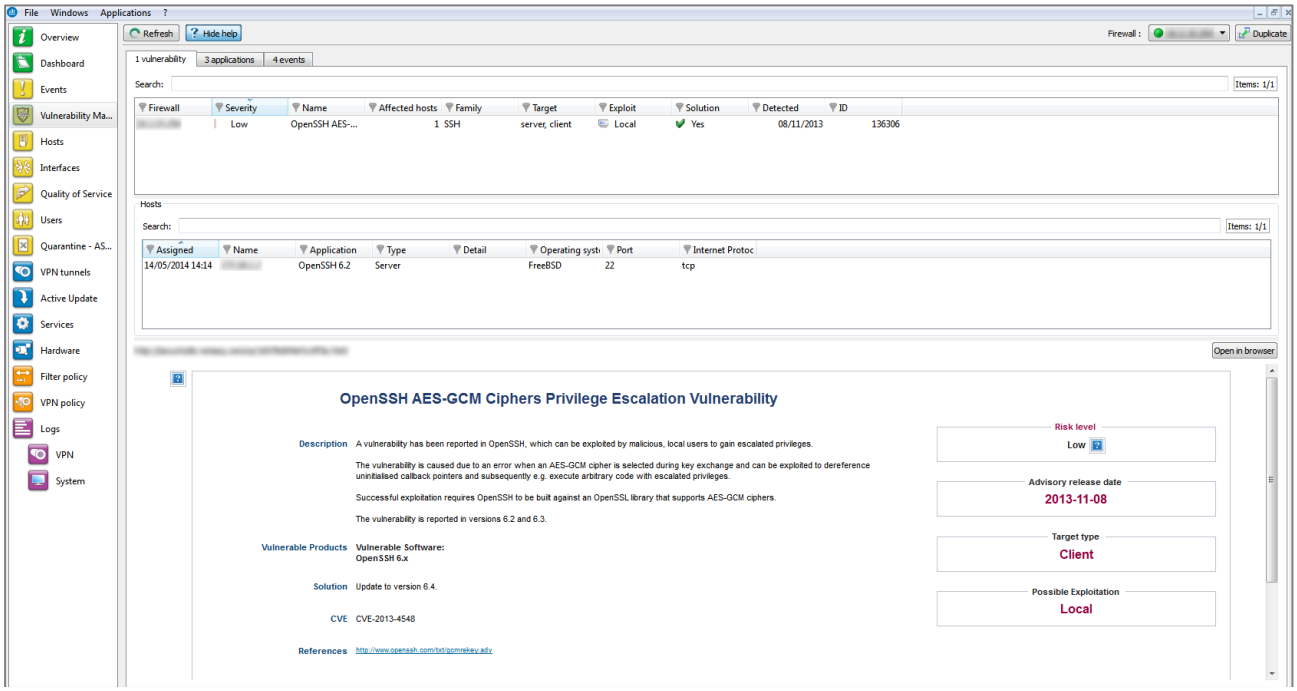


Figure 31: Help

4.2.3 Application tab

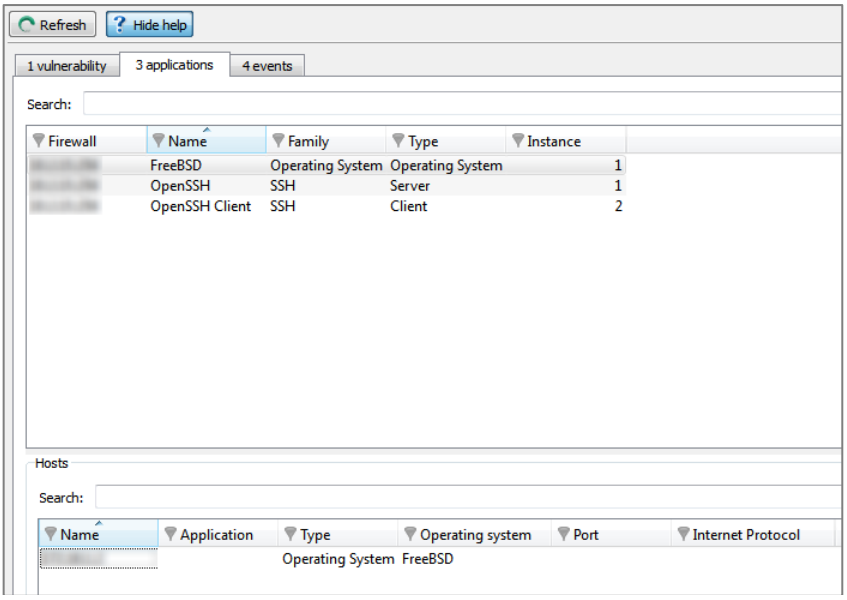


Figure 32: VULNERABILITY MANAGER - Application

The `Applications` tab provides information on the application detected within the enterprise.

Two types of application may be detected:

- **Products**: these are client applications installed on the host (e.g.: Firefox 1.5).
- **Services**: these are server applications that are attached to a port (e.g.: OpenSSH 3.5).

Using information detected by the ASQ engine, Stormshield Network VULNERABILITY MANAGER generates information about the detected applications. The addition of this feature allows grouping applications by family, so by pairing such information with the vulnerability database, SN VULNERABILITY MANAGER also suggests probable security loopholes linked to these applications.

This tab offers features that include filtering, optional column display, resizing to fit contents and copying of data to the clipboard. It displays information on the detected applications through the columns that can be seen in the window above.

The window comprises 2 views:

- A view that lists the applications
- A detailed view that lists the hosts

4.2.3.1 "Application(s)" view

This view allows you to see the applications that the firewall detects. Each line represents an application.

REMARK

The number of applications is displayed in the tab's label.

The **`Applications`** tab displays the following data:

Firewall	Serial number or name (if known) of the firewall.
Name	Name of the software application. The version is not specified except for the operating systems.
Family	The software application's family (e.g.: "web client").
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Instance	Number of software applications detected in the monitored networks. For a server, the same service may be suggested on several ports. E.g.: an Apache http server which provides its services on port 80 and port 8080 (web proxy) would appear twice.

4.2.3.2 "Hosts" view

This view allows you to see all the applications for a given host. Each line represents a host.

The information seen in the "Hosts" view is as follows:

Name	Host name
IP address	IP address of the host
Application	Name of the software as well as its version, if available.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Operating system	Host's operating system.
Port	Port that the software application uses (if it uses any).
Protocol	Internet protocol of the software (if it uses any).

4.2.4 Events tab

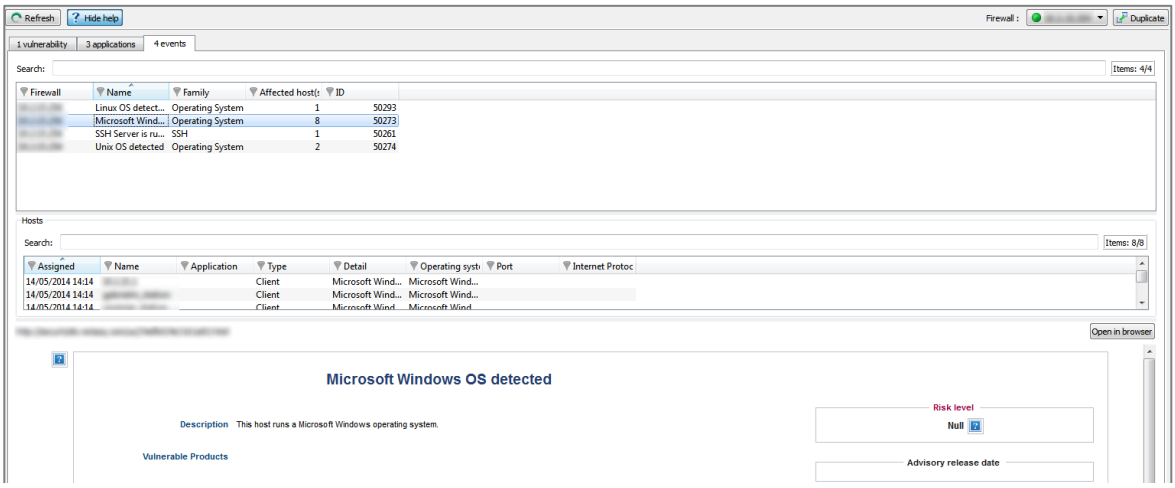


Figure 33: VULNERABILITY MANAGER-Events

The **Information** tab informs you of your network's activity. You can therefore see the programs that are at risk of generating attacks. The window is divided into 3 sections:

- List of programs
- List of hosts
- Help zone
-

4.2.4.1 "Information" view

This view allows you to see all the events that the firewall detects. Each line represents an event.

REMARK

The number of events is displayed in the tab's label.

The "Information" view displays the following data:

Firewall	Serial number or name (if known) of the firewall.
Name	Name of the detected OS or a server (e.g.: SSH server).

Family	Host family. **Example** SSH
Affected hosts	Number of hosts affected. These hosts are identified in the **Hosts** view in this tab. **REMARK** The number of hosts indicated in the column "Affected hosts" is not always the same as the number of elements indicated in the "Hosts" zone in this window. In fact, the same service may use several ports. For example, the service thhtpd_server_2.25b can listen to 2 different ports, thus increasing the number of elements.
Id	Identifier.

4.2.4.2 "Hosts" view

This view allows you to see all the events for a given host. Each line represents a host.

The information seen in the "Hosts" view is as follows:

Assigned	Date and time of the event's occurrence.
Name	Host name.
Address	IP address of the host
Application	Name of the software as well as its version, if available.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service – Operating system).
Detail	Details about the operating system.
Operating system	Host's operating system.
Port	Port that the software application uses (if it uses any).
Internet Protocol	Internet protocol of the software (if it uses any).

4.2.4.3 Help zone

The help zone allows you to get more details relating to the attack. Thus the administrator can correct the vulnerability.

Click on the **Show help** button to show or hide the help zone associated with an event.

Typically, help comes in the form of a descriptive file that contains explanations, links to the publisher's site or to bug fixes.

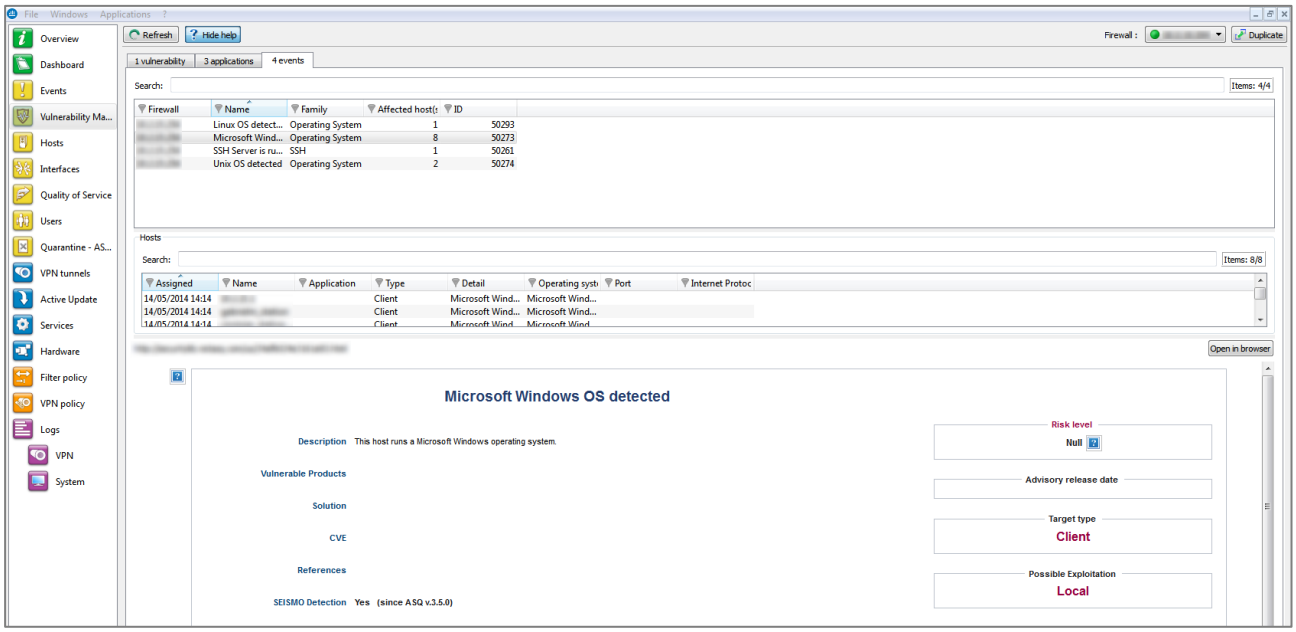


Figure 34: Help

REMARK

Refer to the user guide **Stormshield Network UNIFIED MANAGER** to configure **VULNERABILITY MANAGER**.

4.3 HOSTS

From the menu directory, click on `Hosts`.

This window lists the connected hosts.

4.3.1 "Hosts" tab

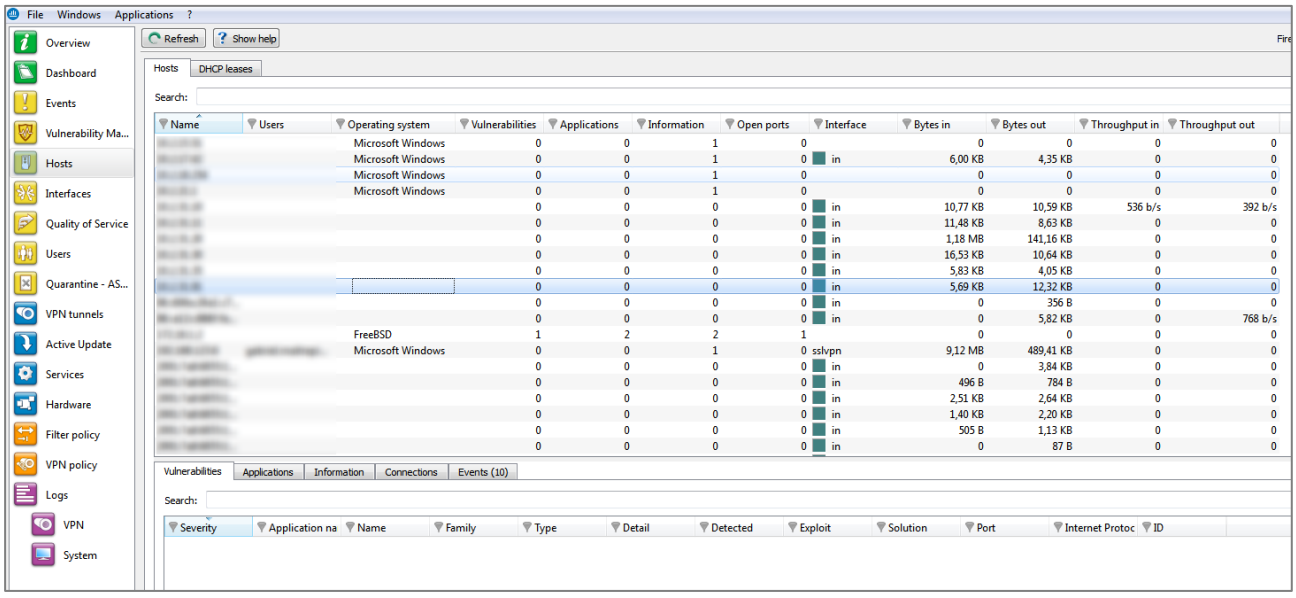


Figure 35: Hosts

The window comprises 3 views:

- A view that lists the hosts
- A view that lists the Vulnerabilities, Applications, Information, Connections and Events relating to the selected host
- A help view that allows working around the selected vulnerability, if a solution exists

4.3.1.1 "Host" view

This view allows you to see all the hosts that the firewall detects. Each line represents a host.

The information seen in the "Hosts" view is as follows:

Name	Name of the source host (if declared in objects) or host's IP address otherwise.
Address	Host's IP address
Users	User connected to the host (if there is one).
MAC address	Host's MAC address.
Operating system	Operating system used on the host.
Information	Indicates the information in the Information tab.
Vulnerabilities	Number of vulnerabilities detected.
Applications	Number of applications on the host (if there are any).
Events	Number of detected events
Open ports	Number of open ports.
Last VULNERABILITY MANAGER event	Indicates the date and time of the last VULNERABILITY MANAGER event.
Interface	Interface on which the host is connected.
Bytes in	Number of bytes that have passed through the Firewall from the source host since startup.
Bytes out	Number of bytes that have passed through the Firewall to the source host since startup.
Throughput in	Actual throughput of traffic to this host passing through the Firewall.
Throughput out	Actual throughput of traffic to this host passing through the Firewall.

4.3.1.2 "Vulnerabilities" view

This tab describes the vulnerabilities detected for a selected host. Each vulnerability can then be viewed in detail.

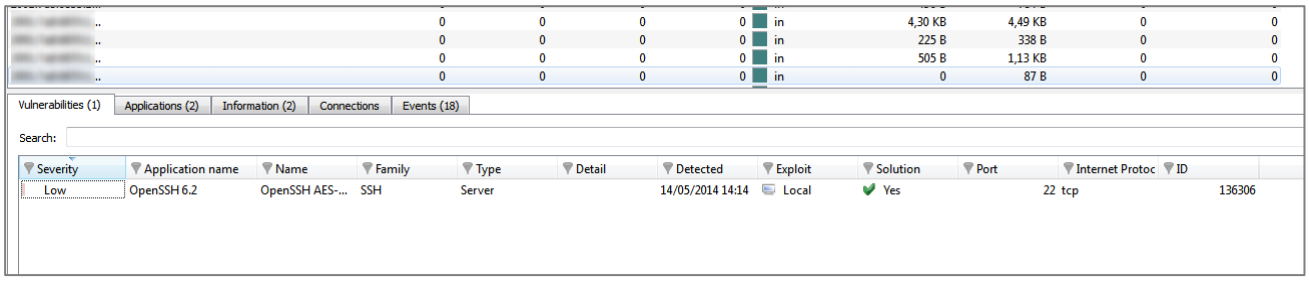


Figure 36: Hosts – Vulnerabilities

The information provided in the "vulnerability" view is as follows:

Firewall	IP address of your Stormshield Network Firewall where the vulnerability comes from.
Severity	Indicates the how severely the host(s) have/has been affected by the vulnerability, according to 4 levels: **Low**, **Moderate**, **High**, **Critical**.
Name	Indicates the name of the vulnerability.
Family	Family to which the vulnerability belongs.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service).
Target	One of 2 targets: **Client** or **Server**.
Affected hosts	Number of hosts affected by the vulnerability.
Exploit	Local or remote access (via the network). Allows exploiting the vulnerability.
Solution	Indicates whether a solution has been suggested.
Date	Date on which the vulnerability was detected. **WARNING** This refers to the discovery date and not the date on which the vulnerability appeared on the network.
Internet Protocol	Name of the protocol used.
Id	Vulnerability identifier.

4.3.1.3 "Applications" view

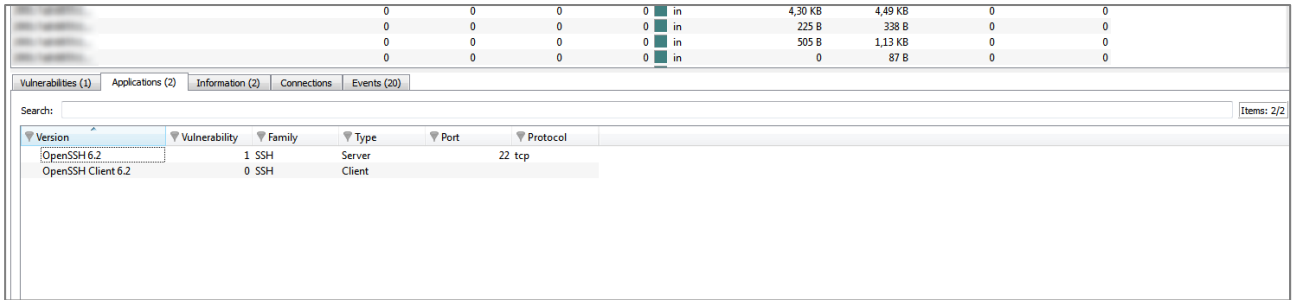


Figure 37: Hosts – Applications

This tab describes the applications detected for a selected host. It is possible to view applications in detail later.

The "Applications" view displays the following data:

Version	Name and version of the application.
Vulnerability	Number of vulnerabilities detected on the application.
Family	The software application's family.
Type	Software type (Client: the software does not provide any service – Server: the software application provides a service).
Port	Port used by the application (if it uses one).
Protocol	Protocol used by the application
ID	Unique identifier of the vulnerability family.

4.3.1.4 "Information" view

This tab describes the information relating to a given host

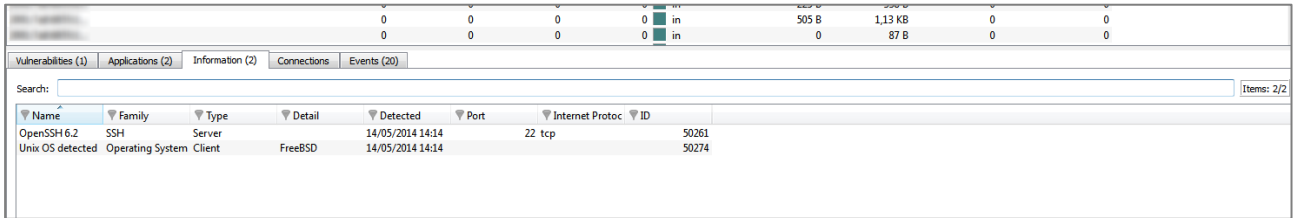


Figure 38: Hosts – Events

REMARK

The number of events is displayed in the tab's label.

The information provided in the "events" view is as follows:

Name	Name of the detected OS.
Family	Family of the vulnerability that is likely to appear (Example: SSH).
Type	Application type (Client: the software does not provide any service – Server: the software application provides a service).
	Name of the detected OS.
Detail	Description of information.
Detected	Date and time of detection.
Port	Number of the port on which the vulnerability had been detected.
Protocol	Name of the protocol used.
Id	Unique identifier of the vulnerability family.

4.3.1.5 "Connections" view

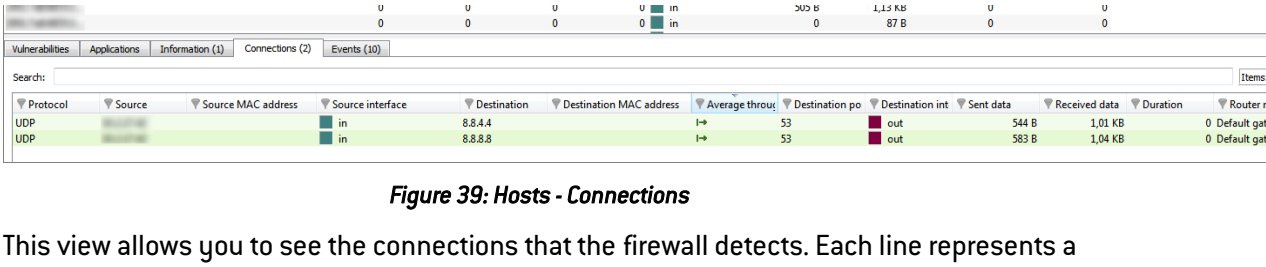


Figure 39: Hosts - Connections

This view allows you to see the connections that the firewall detects. Each line represents a connection.

The "Connections" view displays the following data:

Time	Indicates the date and time of the object's connection.
Protocol	Communication protocol used for the connection.
Source	Name of the object that connected to the selected host.
Source MAC address	MAC address of the object at the source of the connection.
Source port	Indicates the number of the source port used for the connection.
Source interface	Name of the firewall interface on which the connection was established.

Destination	Name of the object for which a connection has been established.
Destination MAC address	MAC address of the object at the destination of the connection.
Average throughput	Average value calculated by the amount of data exchanged divided by the length of the session.
Destination port	Indicates the number of the destination port used for the connection.
Destination interface	Name of the destination interface used by the connection on the firewall.
Data sent	Number of bits sent during the connection.
Data received	Number of bits received during the connection.
Duration	Connection duration.
Router	Identifier that the firewall assigned to the router used by this connection
Router name	Name of the router saved in the object base used by the connection
Policy	Name of the policy that allowed the connection
Rule	Name of the identifier of the rule that allowed the connection
Operation	Identified command of the protocol.
Parameter	Operation parameter.
Status	This parameter indicates the status of the connection corresponding, for example, to its initiation, establishment or closure.

4.3.1.6 "Events" view

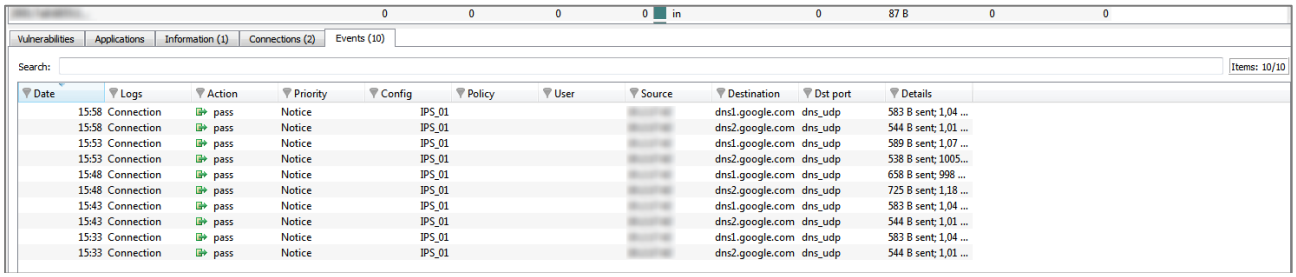


Figure 40: Hosts - Events

This view allows you to view all the events that the firewall has detected. Each line represents an alarm.

The information provided in the "Events" view is as follows:

Date (time)	Date and time the line was recorded in the log file at the firewall's local time.
UTC Date (time+tz)	UTC date (replaces the GMT)
Start date (starttime)	"Local" date at the start of an event.
UTC start date (startime+tz)	UTC date at the start of an event (a connection).
Timezone (tz)	Firewall's timezone at the time the log was written.
Logs	File at the source of the event.
Action (action)	Action associated with the filter rule and applied on the packet (**Examples**: Block/Pass…)
Priority (pri)	Determines the alarm level. The possible values are:

	0: emergency 1: alert 2: critical 3: error 4: warning 5: notice 6: information 7: debug
Rule (ruleid)	Number of the filter rule involved in the raised alarm.
Config	Name of the application inspection profile that reported the event.
Policy	Name of the SMTP, URL or SSL filter policy that raised the alarm.
User	Identifier of the user requesting authentication
Protocol (proto)	Protocol of the packet that set off the alarm.
Connection group (groupid)	Identifier that would allow tracking child connections.
Source interface (srcif/srcifname)	Network card of the source interface (name of the source host or the object corresponding to the service port of the source machine if it exists).
Source (src)	IP address or name of the object corresponding to the source host of the packet that set off the event.
Source address (src)	IP address of the source host of the packet that set off the event.
Source MAC address	MAC address of the object at the source of the connection.
Source port (srcport)	Port number of the source (only if TCP/UDP).
Destination interface (dstif)	Network card of the destination interface.
Destination (dst/dstname)	IP address or name of the object corresponding to the destination host of the packet that set off the event.
Destination address (dst)	IP address of the destination host or name of the object corresponding to the IP address (if it exists) of the packet that set off the event.
Destination port (dstport/dstportname)	Port requested for this connection.
Details	Describes the event relating to the log. This description groups together information from other columns in a single column. *Example: if it is an alarm log, information such as whether the alarm is sensitive, the filter rule number and rule identifier will be indicated in this column or will otherwise be new columns in order to enable filtering.* *Please refer to the "Description of Audit logs" technical note.*

For the description of additional data available by column title, please refer to the chapter **4.1. EVENTS**.

4.3.2 "DHCP leases" tab

This tab displays all hosts that have a lease in progress or which has ended and specifies the state of this lease. The information provided in the "DHCP leases" tab is as follows:

IP Address	Host's IP address
Name	Name of the host that have a lease in progress or which has ended (if declared in objects) or host's IP address otherwise.
Status	The status of the lease can be: • **Active:** the address has been assigned to a host and the assignment is still in progress. • **Free:** the lease has expired, and the address can be reused for another lease.
From	Starting date and time of the bail assignment.
Until	Ending date and time of the bail assignment. This can be a date and time in the past or future
Mac address	Physical network identifier of the host with an ongoing or lapsed lease.

REMARK

The leases assigned by reservation (static IP address reserved exclusively for a MAC address) are not displayed in this screen.

REMARK

When a new host logs on to a network, it will send a first request (DHCPDISCOVER) to the whole network to find out where the DHCP servers are. Upon reception, the DHCP server will pre-reserve an IP address and sends it to the host (DHCPOFFER). It is possible, however, that this host already uses the address range of another DHCP server. During this pre-reservation period (2 minutes), the IP address will no longer be available but will appear in the list as "free". If many pre-reservations are made within a short period, the server may run out of available addresses while the screen continues displaying "free" addresses.

4.4 INTERFACES

4.4.1 Introduction

DEFINITION

A zone, whether real or virtual, that separates two elements. The interface thus refers to what the other element need to know about the other in order to operate correctly.

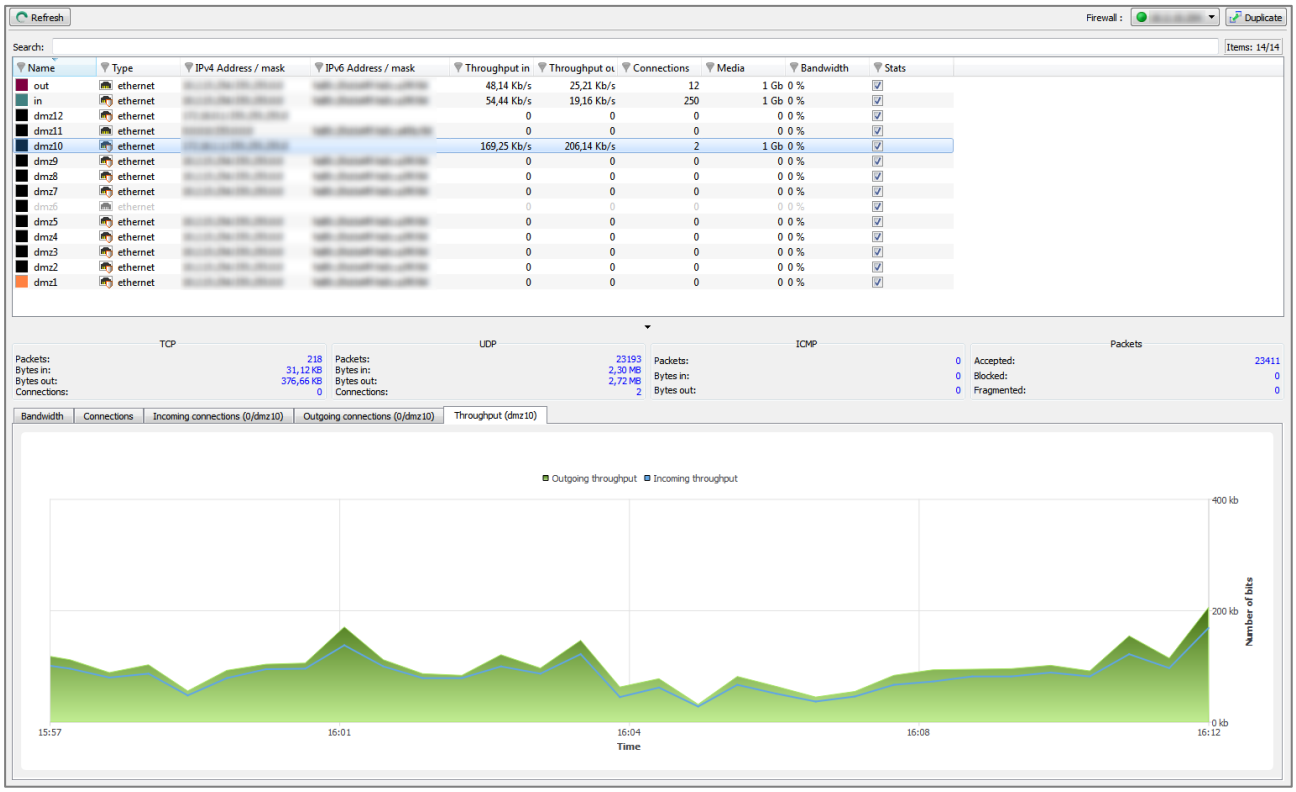


Figure 41: Interfaces

The **Interfaces** menu presents different statistics concerning:

- Bandwidth
- Connections
- Throughput
- Statistics are displayed in the form of graphs. The vertical and horizontal axes are graduated. The horizontal axis represents time, and the vertical axis is either:
- Bandwidth percentage
- The number of connections, or
- Throughput expressed in bytes, kilobytes or megabytes.

4.4.1.1 Interface types

- Vlan.
- Ethernet.
- PPTP.
- Dialup.

REMARK

The interfaces are grayed out or do not appear at all when they are inactive.

The window consists of 3 views:

- A view of the interfaces in tables (or legend)
- A details zone
- A zone for viewing graphs

4.4.2 Legend view (or tabular view of interfaces)

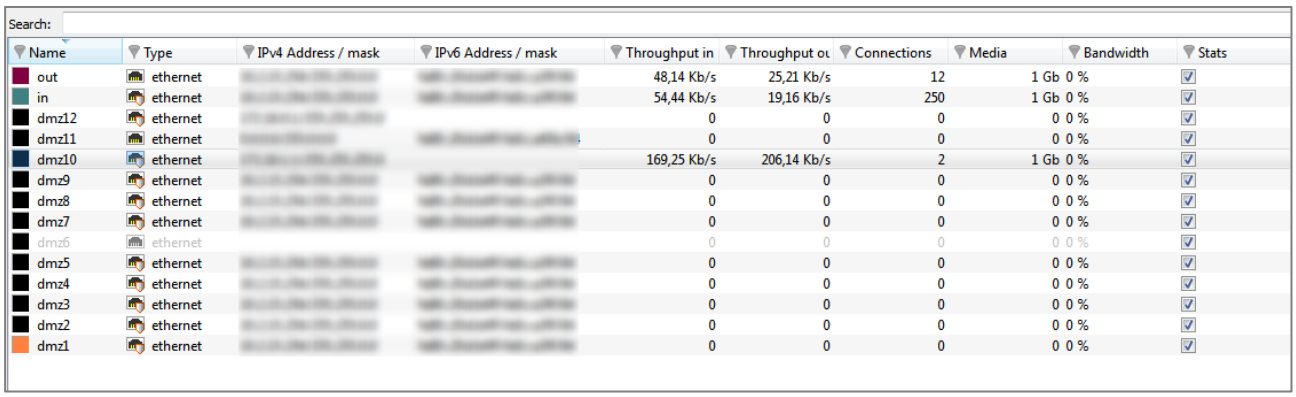


Figure 42: Interfaces – Legend

This view allows you to view all the interfaces that the firewall has detected. Each line represents an interface.

The information provided in the "legend" view is as follows:

Name	Name and color attributed to the interface. The colors allow you to distinguish the interface in the different graphs.
Type	Type of interface with a matching icon.
IPv4 Address/ Mask	IPv4 address and subnet mask of the interface.
IPv6 Address/ Mask	IPv6 address and subnet mask of the interface.
Throughput in	Indicates the real incoming throughput.
Throughput out	Indicates the real outgoing throughput.
Connections	Number of real-time connections on each interface of the firewall over a defined period.
Media	By default, its value is 0. The throughput of a network interface can be configured via **UNIFIED MANAGER**.
Bandwidth	Indicates the percentage of bandwidth used for an interface.
Stats	If this option is selected, the graph corresponding to this interface will be displayed.

REMARK

Inactive interfaces are grayed out.

You will notice the colors of the visible interfaces at the top of the window. These colors are defined in the network parameters of the **Stormshield Network UNIFIED MANAGER** for each interface (refer to the **Stormshield Network UNIFIED MANAGER** *user manual*).

4.4.3 "Details" view

Each chart provides statistical information on throughput for each interface:

- Name, IP address, subnet mask (American format – see Appendix for explanations), connection type (10 or 100Mbits, half duplex or full duplex),
- Instantaneous (left) and maximum (right) throughput,
- Number of packets and volume in bytes for TCP, UDP and ICMP,
- Number of TCP connections,
- Total number of packets accepted, blocked and fragmented by the Firewall.

4.4.4 "Bandwidth" tab

The bandwidth graph displays the percentage of use of the available bandwidth on each interface in real time.

Figure 43: Interfaces - Bandwidth

Each interface is represented by a different color of which the legend may be found at the top of the graph. Maximum bandwidth represents the theoretical maximum throughput supported by the interface.

> **Example**
>
> For a 100Mbits/s line used in full duplex, this maximum is 200 Mbits/s, and for a 10Mbits/s line used half duplex it is 10 Mbits/s.

4.4.5 "Connections" tab

The connection graph displays in real time the number of connections on each of the Firewall's interfaces during the defined period.

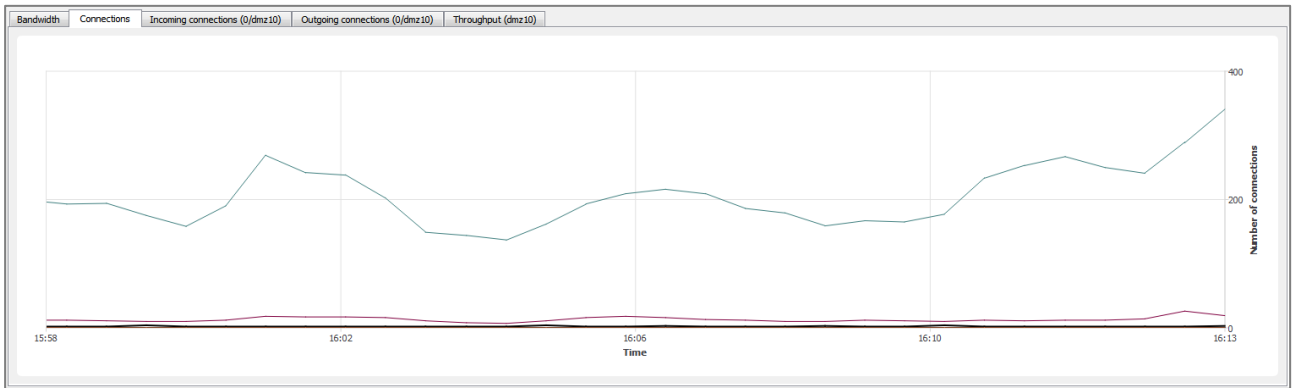


Figure 44: Interfaces - Connections

Each interface is represented by a different color of which the legend may be found at the top of the graph.

4.4.6 "Incoming connections" tab

The screen displays incoming connections in progress relating to the selected interface. To find out what data are offered, please refer to the chapter of the **Hosts** module, section **"Connections"** view for the hosts tab.

4.4.7 "Outgoing connections" tab

The screen displays outgoing connections in progress relating to the selected interface. To find out what data are offered, please refer to the chapter of the **Hosts** module, section **"Connections"** view for the hosts tab.

4.4.8 "Throughput" tab

The throughput graph represents the real throughput on each of the Firewall's interfaces. The throughput scale automatically adapts to the maximum throughput recorded during the period.

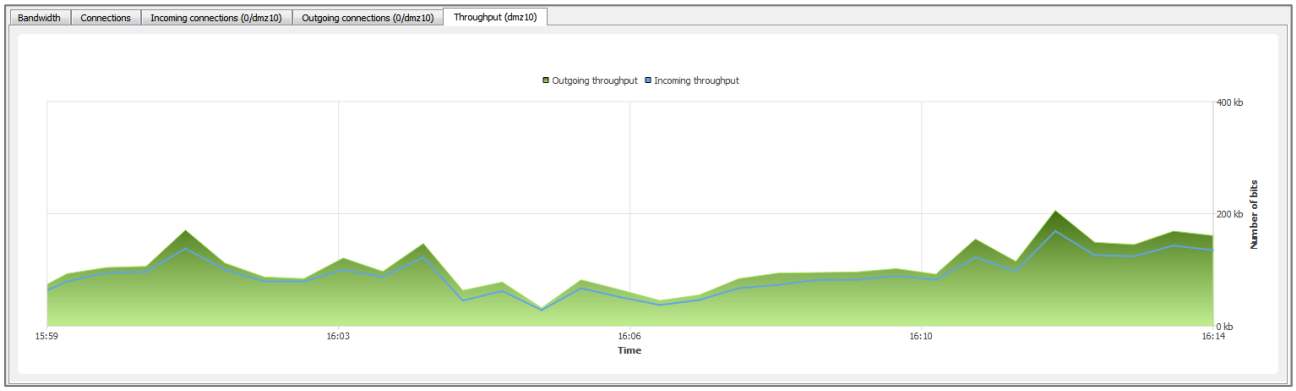


Figure 45: Interfaces - Throughput

For each interface, the throughput graph indicates the ingoing and outgoing throughput.

To modify the interface on which throughput is viewed, click on this interface in the legend at the top right section of the graph. The interface currently being viewed will be highlighted in blue.

4.5 QUALITY OF SERVICE (QoS)

REMARKS

1) Quality of Service, which has a high level of abstraction, refers to the ability to provide a network service according to parameters defined in a Service Level Agreement (SLA). The "quality" of the service is therefore gauged by its availability, latency rate, fluctuations, throughput and rate of lost packets.
2) Where network resources are concerned, the "Quality of service" refers to a network element's ability to provide traffic prioritization services and bandwidth and latency time control.

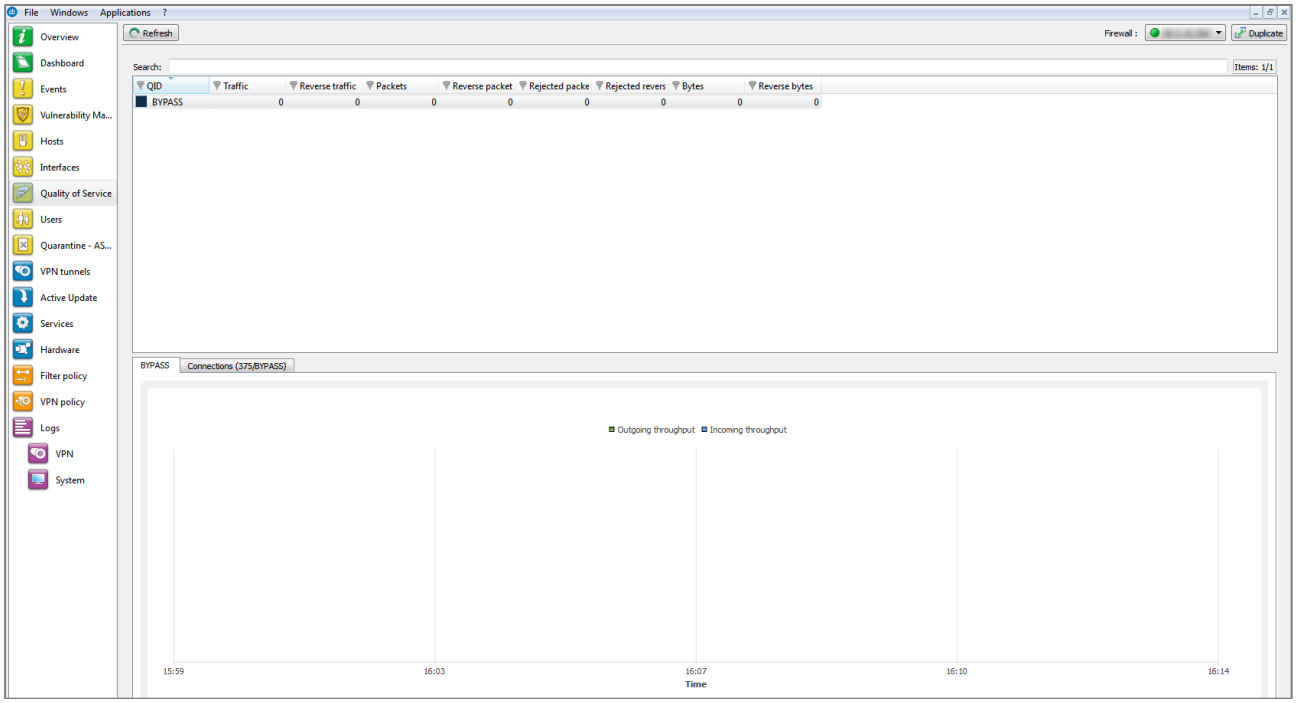


Figure 46: Quality of service

This window consists of 2 views:

- A table view
- A graph view

The following data is displayed when you click on the **Quality of service** menu:

QID	Name of the policy defined for accepting or rejecting packets.
Traffic	Indicates in real time the incoming throughput that the QID manages.
Reverse traffic	Indicates in real time the outgoing throughput that the QID manages
Packets	Number of incoming packets in real time over a defined period.
Reverse packets	Number of outgoing packets in real time over a defined period
Rejected packets	Number of rejected incoming packets on the network.
Rejected reverse packets	Number of rejected outgoing packets.
Bytes	Value in Kbits or Mbits.
Reverse Bytes	Value in Kbits or Mbits.

4.5.1 "Diagram" view

This view shows the incoming and outgoing throughput associated with the different QIDs defined on the firewall's QoS policy.

4.5.2 "Connections" view

The *Connections* tab displays connections in progress going through the selected queue. To find out what data are offered, please refer to the chapter of the **Hosts** module, section **"Connections"** view for the hosts tab.

4.6 USERS

4.6.1 Introduction

The **User** menu enables viewing, in the capacity of an administrator, the users who are currently connected on the Firewall.

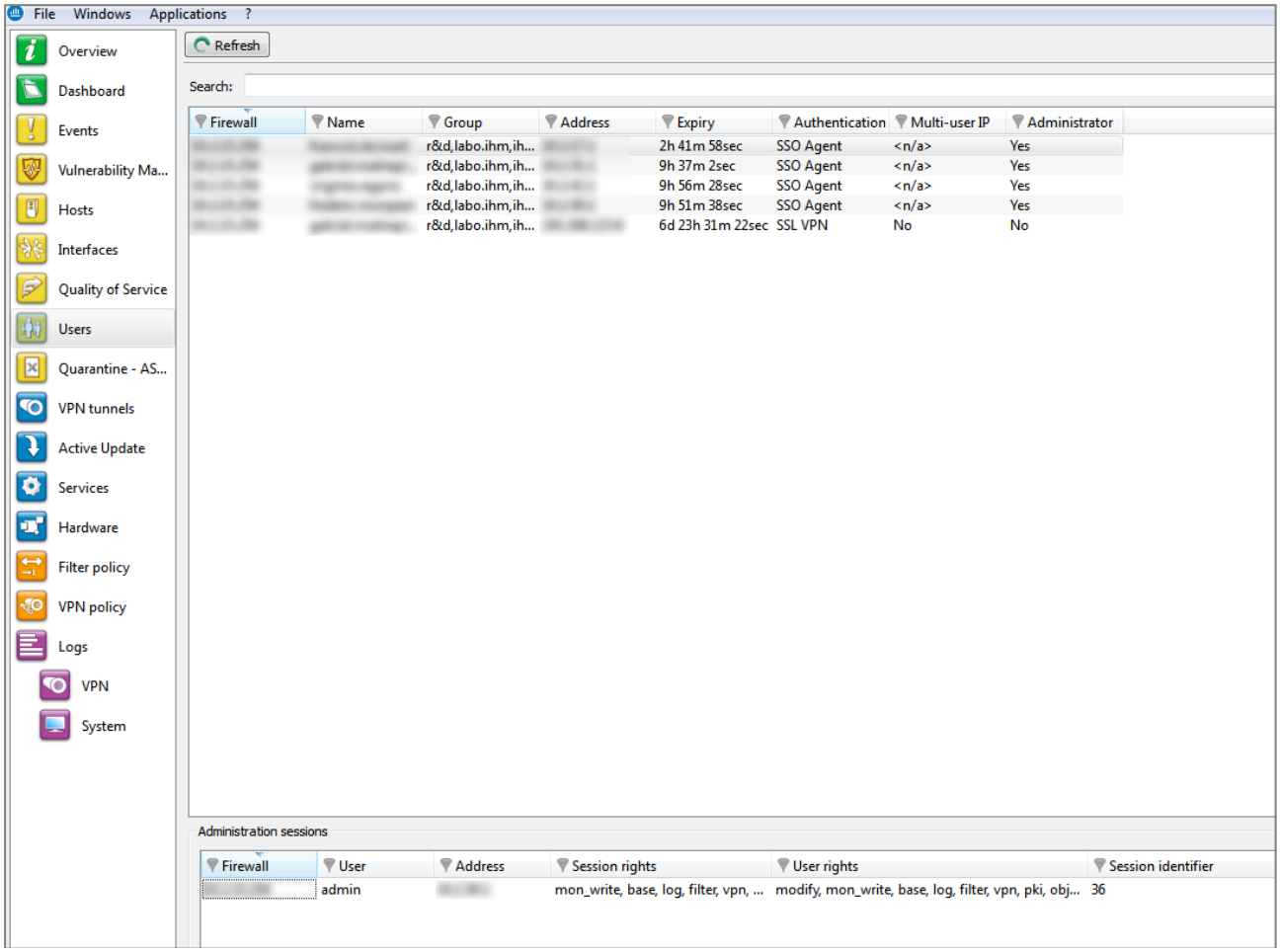


Figure 47: Users

This window comprises 2 views:

- A "users" view.
- An "administration session" view.

4.6.1.1 "Users" view

The information provided in the "users" view is as follows:

Firewall	Serial number or name (if known) of the firewall.
Name	Name of authenticated user.
Group	Name of the group to which the user belongs.
Address	User's IP address.
Timeout	Time remaining for this authentication session (a user is authenticated only for a limited duration).
Authentication	Authentication method used.
Multi-user IP	Indicates whether multi-user authentication is used (one IP address shared by several users). REMARK As the SSO Agent method only allows one authentication per IP address, the value will therefore not be available (value <n/a> displayed).
Administrator	Indicates the type of 'Administrator" privileges granted to the connected user.

4.6.1.2 "Administration sessions" view

This window enables finding out the session privileges of the user connected to the firewall.

The information provided in the "administration sessions" view is as follows:

Firewall	Serial number or name (if known) of the firewall.
User	Authenticated user's identifier.
Address	IP address of the connected user's host.
Session privileges	Indicates the privileges for the current session. Only one administrator is allowed to make changes in each session (*modify* and *mon_write* privileges).
User privileges	Indicates privileges that have been given to the connected user (these privileges include adding, modifying, deleting or reading in different applications).
Session identifier	Number identifying the session.

4.7 QUARANTINE – ASQ BYPASS

DEFINITIONS

1) **Dynamic quarantine**: the quarantine is manually done and for a set duration.
2) **Static quarantine**: the quarantine is automatic and for permanent. Static quarantining is configuring in the application **Stormshield Network UNIFIED MANAGER**.

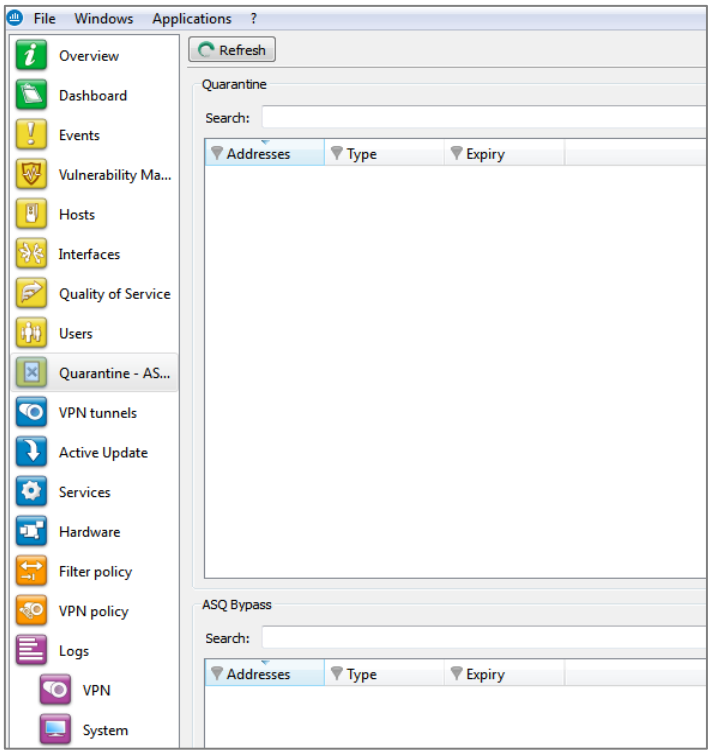


Figure 48: Quarantine

This window comprises 2 views:

- A "Quarantine" view
- An "ASQ Bypass" view.

4.7.1 "Quarantine" view

This window shows the hosts that have been dynamically quarantined. Hosts in static quarantine are not reflected in this list. The information provided in the "Quarantine" view is as follows:

Addresses	IP address of the host(s) affected by the quarantine.
Type	2 options are possible: **Host to host** and **Host to all**.
Expiry	Time at which the quarantine will expire.

4.7.2 "ASQ Bypass" view

The information provided in the "ASQ Bypass" view is as follows:

Addresses	IP address of the host(s) affected by the ASQ Bypass.
Type	2 options area possible: **Host to host** and **Host to all**.
Expiry	Time at which the ASQ Bypass will expire.

5 NETWORK ACTIVITY

5.1 VPN TUNNELS

The VPN Tunnels module presents IPSec VPN and SSL VPN tunnels under two separate tabs.

5.1.1 IPSec VPN Tunnels tab

The following window appears when you click on the **VPN Tunnels** menu:

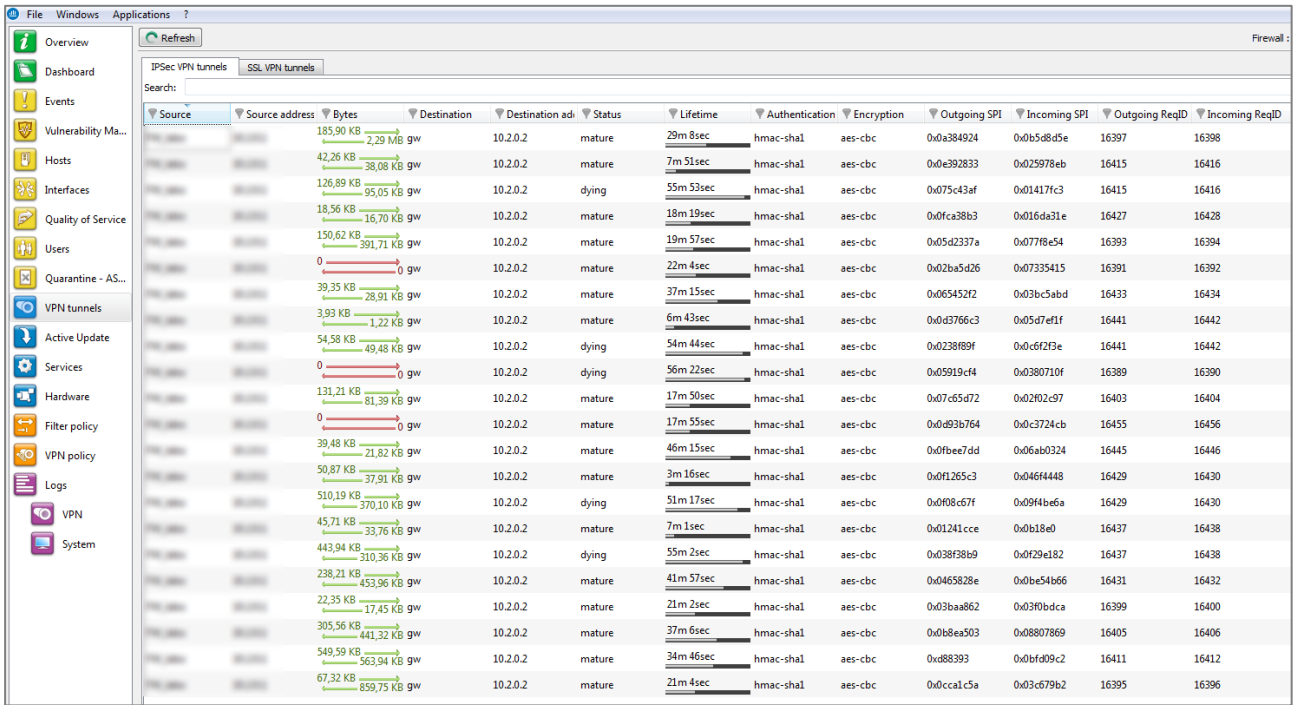


Figure 49: IPSec VPN tunnels

Here, you will see statistical information on the tunnel's operation.

The data displayed in this window are as follows:

Source	IP address or name of the tunnel initiator
Source address	IP address of the tunnel initiator
Bytes	Indicates incoming and outgoing throughput.
Destination	Destination IP address
Status	Indicates the tunnel's status. (Example: Mature).
Lifetime	The SA's (Security Association) lifetime in a graphical representation of the position in this lifetime as well as the value (expressed in hours, minutes and seconds)
Authentication	The authentication algorithm
Encryption	Name of the encryption algorithm

The tunnel is made up of two sub-tunnels, one for each direction of the datagram transmission.

REMARK

The algorithms and limits have been configured in the **Stormshield Network UNIFIED MANAGER** (refer to the Manager user and configuration guide help for further details).

TIP

You will find other information on the parameters in this window in the RFC.

Further information may be found in RFC 2401 IPSEC:

http://www.ietf.org/rfc/rfc2401.txt

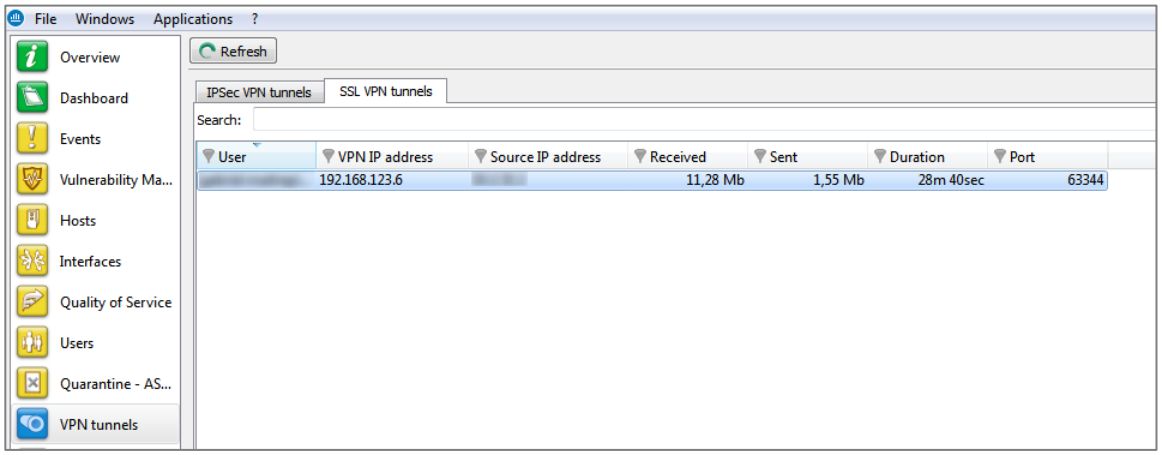
or on sites such as: http://www.guill.net/reseaux/Ipsec.html

This status is color-coded. The line containing VPN information will use the color corresponding to the tunnel's status.

	Undetermined.
	Larval: the SA is in the process of being negotiated or has not been completely negotiated.
	Mature: the SA has been established and is available; the VPN tunnel has been correctly set up.
	Dying: the SA will soon expire; a new SA is in the progress of being negotiated.
	Dead: the SA has expired and cannot be used; the tunnel has not been set up and is therefore no longer active.
	Orphan: a problem has arisen, in general this status means that the tunnel has been set up in only one direction.

5.1.2 SSL VPN Tunnels tab

By clicking on the SSL VPN tunnels tabs in the **VPN Tunnels** menu, the following screen will appear:



It displays statistics on the operation of SSL VPN tunnels that have been set up.

The data displayed in this window are:

User	Name of the user that initiated the tunnel.
VPN IP Address	IP address assigned by the OpenVPN server to the client, for communications through the SSL VPN tunnel.
Source IP Address	IP address of the client workstation outside the SSL VPN tunnel (local network address).
Received	Amount of data the client has received through the SSL VPN tunnel (unit: bits).
Sent	Amount of data the client has sent through the SSL VPN tunnel (unit: bits).
Duration	Time elapsed since the setup of the SSL VPN tunnel (expressed in days, hours, minutes and seconds).
Port	Source port used by the client to set up the SSL VPN tunnel.

5.2 ACTIVE UPDATE

DEFINITION: ACTIVE UPDATE

Enables updating the antivirus database, ASQ contextual signatures, the list of antispam servers, trusted root certification authorities and the URLs used for dynamic URL filtering.

This window displays the status of Active Update on the firewall for each type of update available (Antispam, Antivirus, Contextual signatures, Root certificates, Dynamic URL).

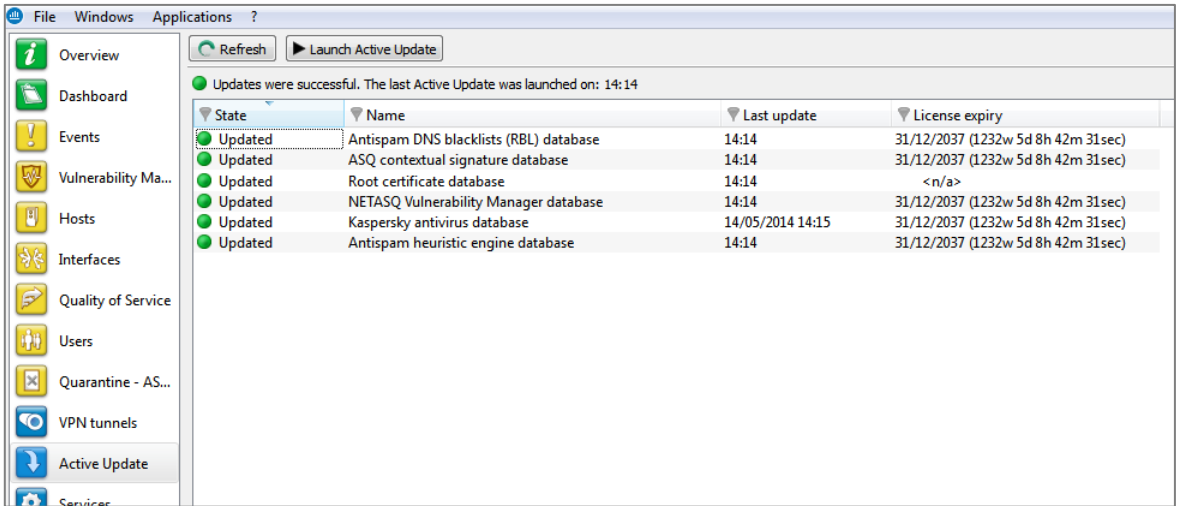


Figure 50: Active Update

Active Update is used for automatically keeping URL databases up to date by downloading them on servers such as updateX. stormshield.eu.

The Monitor screen indicates the result of the last update (successful or failed) and the date of the last update.

The following data will be displayed when you click on the **Active Update** menu:

Status	Indicates the status of the Active Update. 2 options are possible: **The last update failed** / **Updated**.
Name	Indicates the update data categories.
Last update	Indicates the date and time of the last update.
License expiry	Indicates the expiry date of the license option for this category.

5.3 SERVICES

This window sets out the services (active and inactive) on the Firewall and for how long they have been active/inactive.

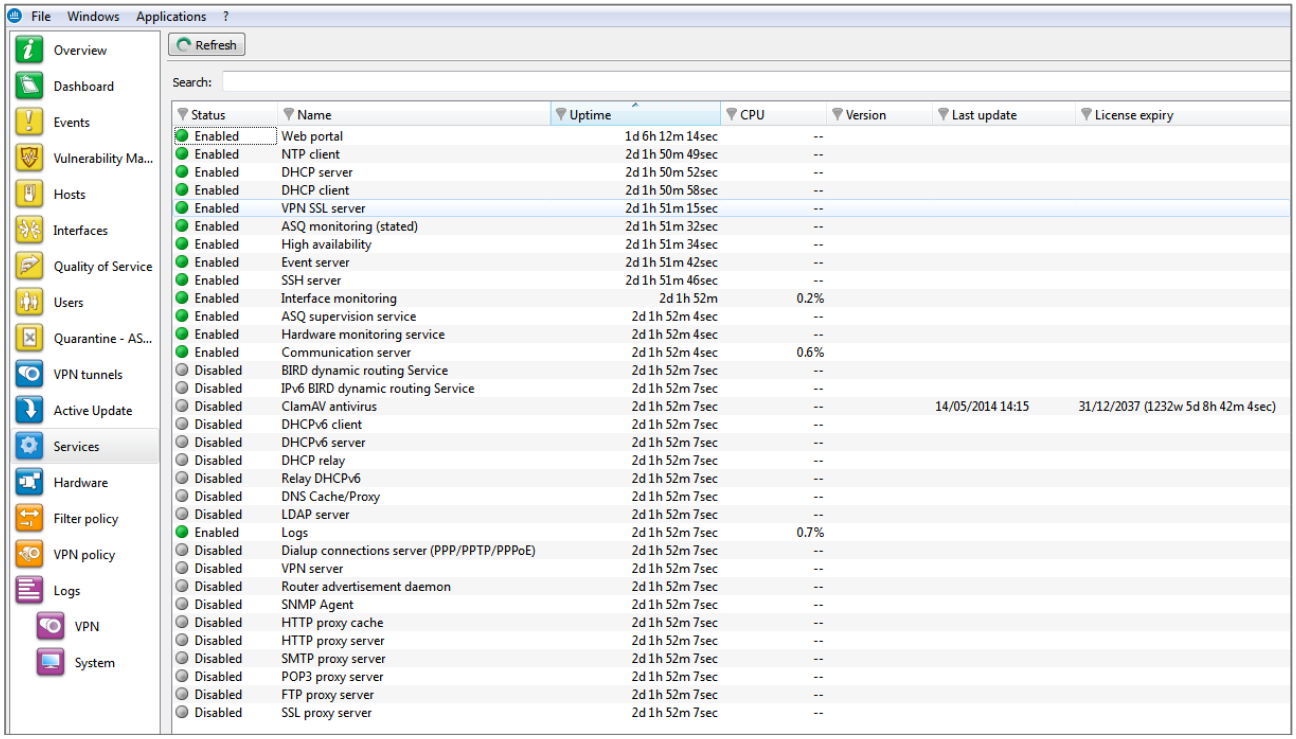


Figure 51: Services

Proxies are displayed in 4 distinct entries:

- HTTP Proxy
- SMTP Proxy
- POP3 Proxy
- FTP Proxy

Information regarding antivirus can also be seen in this window (activity, version, last update, expiry of its license).

The following data will be displayed when you click on the **Services** menu:

Status	Indicates whether services are active or inactive.
Name	Indicates the names of services.
Uptime	Indicates the number of number of days the service has been running and the time of activation.
CPU	Portion of processor resources used by the service (percentage).
Version	Version number of the service.
Last update	Date of the last time the service was updated.

5.4 HARDWARE

5.4.1 High availability

This window displays information concerning the initialization of high availability.

DEFINITION OF HIGH AVAILABILITY

High availability is an option that allows two firewalls (identified through a MasterHA and BackupHA license) to exchange information on their statuses, via a dedicated link in order to ensure service continuity in the event one of the firewalls breaks down. Firewalls in high availability have the same configuration – only their serial numbers, licenses (Master or Backup) and most of all, their status (active or passive) differ.

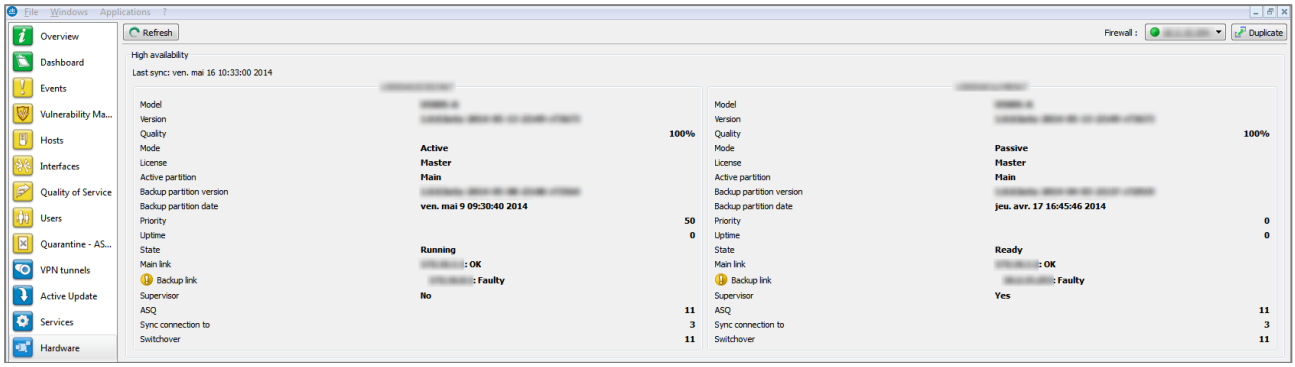


Figure 52: Hardware

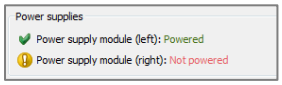
NOTE

Version 1.0 of Stormshield Network multifunction firewalls allows you to benefit from high availability support and a new-generation display with the date of the last synchronization.

You will also notice changes to RAID support.

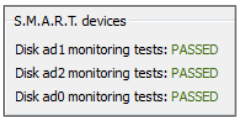
5.4.2 Power supplies

If your firewall model supports redundant power supply modules (high-end models SN3000 and SN6000), the power supply statut will be displayed.



5.4.3 S.M.A.R.T. devices

The result of monitorng tests that have been conducted will be displayed for each S.M.A.R.T. peripheral detected.



5.4.4 RAID

The following is the information relating to the status of RAID volumes and the disks that it comprises:

Disk type	Indication of the type of RAID volume or type of disk that makes up a RAID volume. Example: Mirrored array (Raid1) for a RAID volume.
Disk address	Physical location of the disk contributing to a RAID volume. Example: Upper slot.
Disk status	Status of the RAID volume or of a disk that it comprises. Example: Degraded, Optimal.

5.4.5 Log Storage Disks

The information relating to the storage medium is:

Type	Indicates the type of storage medium.
ID	Identifier of the storage medium (assigned by the firewall).
Status	Indicates whether the storage medium is recognized.
Disk space	For formatted media, this indicates the size of the partition in Gigabytes.
Formatted	Indicates whether the storage medium is formatted.

In the event of a problem with a disk, a message will be displayed in the dashboard.

6 POLICIES

6.1 FILTER POLICY

The **Filter Policy** menu, accessible from the menu directory, in Monitor recaps the active filter policy by grouping together implicit rules, global filter rules and local filter rules.

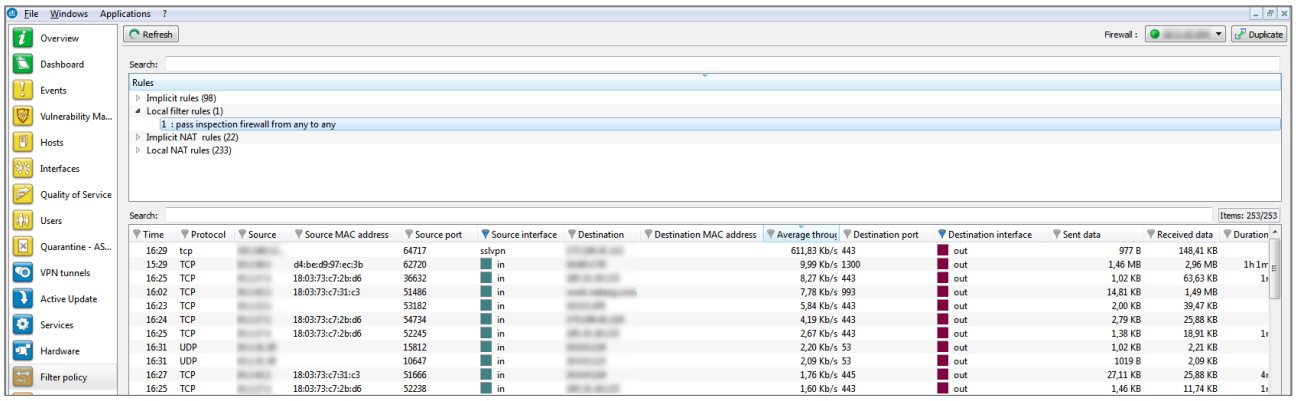


Figure 53: Filter policy

Each row displayed is set out as follows:

```
<identifier for the rule type >: <identifier for the rule in the slot>: <filter rule>
```

Where

- <identifier for the rule type > can be “0” for implicit rules, “1” for global filters and “2” for local filters.
- <identifier for the rule in the slot>: this identifier is always “0” for implicit rules.
- <filter rule>: filter rule created by Stormshield network.

6.1.1.1 “Connections” view

The “*Connections*” view sets out for each rule, all the connections allowed by the implicit, local and global filter policies.

6.2 VPN POLICY

Definition VPN (*Virtual Private Network*)

The interconnection of networks in a secure and transparent manner for participating applications and protocols – generally used to link private networks to each other through the internet.

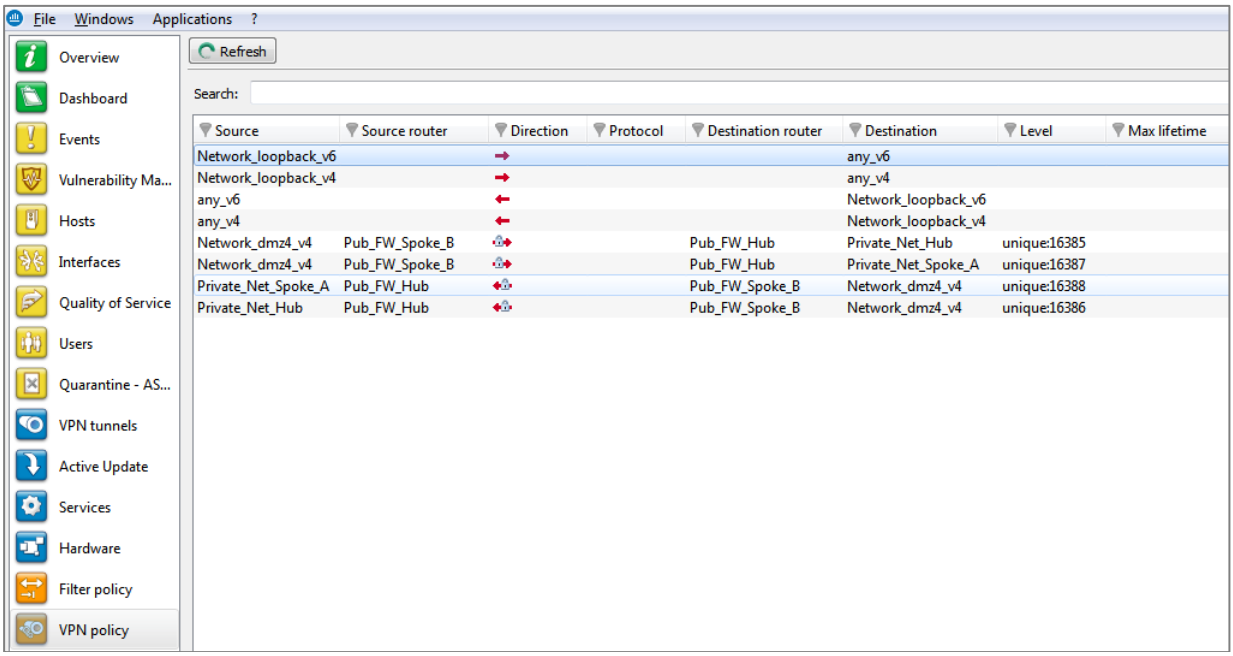


Figure 54: VPN policy

The VPN section allows viewing the configuration of different VPN tunnel policies defined in the active VPN slot. These VPN policies do not necessarily have to be used in order to be displayed. The VPN slot only needs to be activated.

The following information is displayed in this window:

Source	Traffic endpoint. Indicates the source network.
Source router	Indicates the address of the source gateway.
Direction	Indicates the direction of the traffic represented by the following icons: •  •  •  • 
Protocol	Indicates the protocol(s) allowed to pass through the tunnel.
Destination router	Indicates the address of the destination address.
Destination	Traffic endpoint. Indicates the destination network.
Level	Level of security associated with the tunnel. **REMARK** This level is defined when creating the VPN tunnel according to the encryption and authentication algorithm).
Max lifetime	Maximum lifespan of the configured VPN policy.

7 LOGS

7.1 STATUS OF USE

A graph represents the current size of the log file in real time ("Alarms", "Authentication", "Connections", "Filters", "ftp", "Monitor", "Plugins", "POP3", "VULNERABILITY MANAGER", "Administration", "SMTP", "System", "IPSec VPN", "Web", "SSL VPN") in relation to the size allocated on the Firewall for each log type.

DEFINITION OF LOGS

Chronological record of a computer's activity, which makes up a journal of events that took place in programs and systems over a given period.

7.2 LOG TYPES

7.2.1 VPN

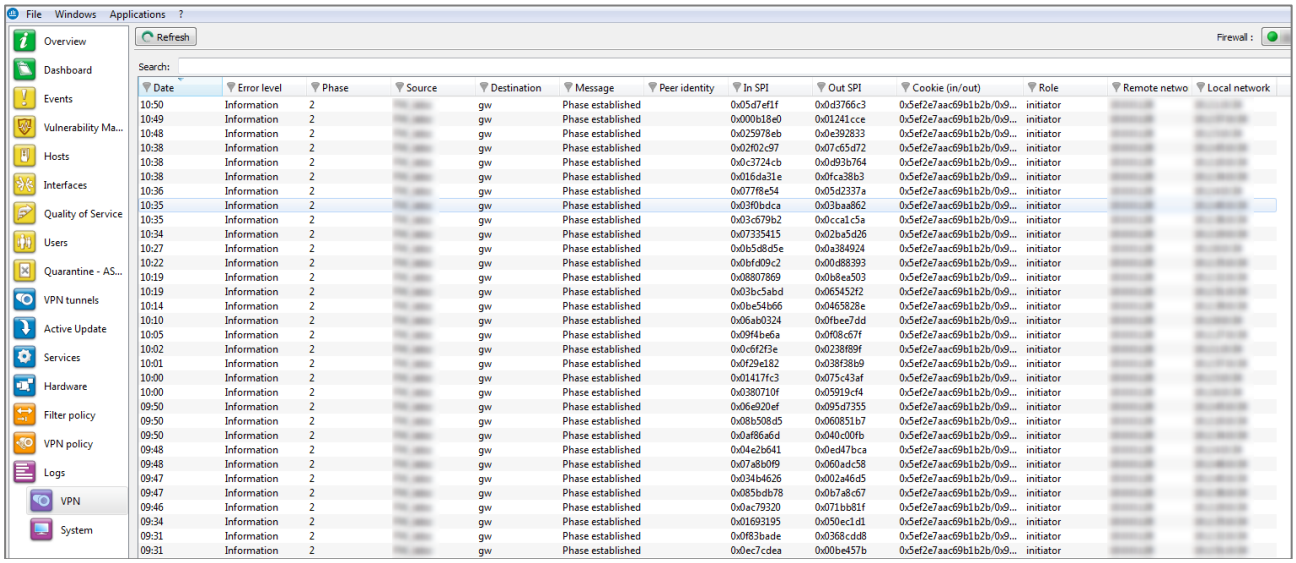


Figure 55: VPN

The following data is displayed when you click on the **VPN** menu:

Date	Date and time the entry was generated
Error level	Error message
Phase	SA negotiation phase
Source	Connection source address (tunnel initiator).
Destination	Destination IP address or name
Message	Message informing of an attempt to set up a tunnel.
Peer identity	Identity of the peer indicated in pre-shared key configuration where "IP address" has not been specified as the identity type.

In SPI	SPI number of the negotiated incoming SA (in hexadecimal).
Out SPI	SPI number of the negotiated outgoing SA.
Cookie (incoming outgoing)	Temporary identity markers for the initiator and recipient of the negotiation.
Role	Indicates the user's endpoint.
Remote network	IP address of the remote network on the traffic endpoint.
Local network	IP address of the local network on the traffic endpoint.

7.2.2 System

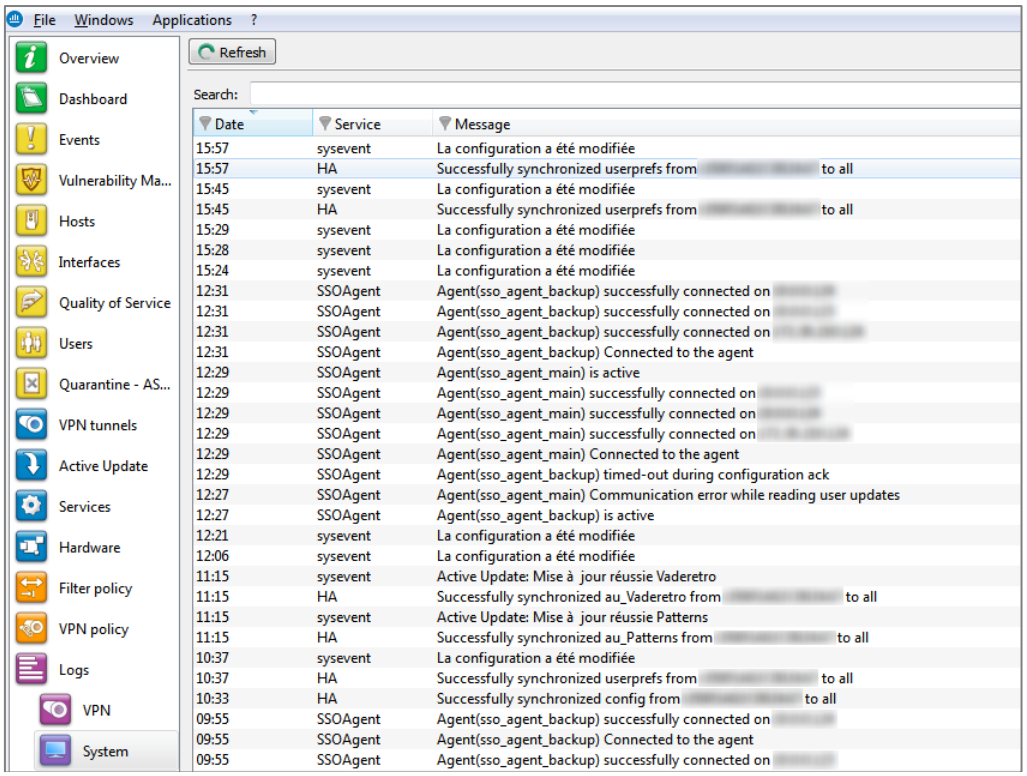


Figure 56: System

The following data is displayed when you click on the **System** menu:

Date	Date and time entry was generated
Service	Name of the service
Message	Indicates the action applied.

APPENDICES

Appendix A: FAQ

1). what is the meaning of the message “Impossible to locate the machine on x.x.x.x”?

2). How can I check the IP address (es) really assigned to the Firewall?

3). what is the meaning of the message ‘You lost the MODIFY privilege’?

4). what is the meaning of the message ‘The operation has exceeded the allotted time’?

5). How do I know if there has been an attempted intrusion?

6). It is possible to allow protocols other than IP?

1) What is the meaning of the message “Impossible to locate the machine on x.x.x.x”?

This message means that the host on which you are connected cannot reach the Firewall by the IP address you have specified in the connection window. This may be for one of several reasons.

Check:

- That the IP address which you have specified in the connection window is that of the Firewall (that of the internal interface in advanced mode),
- That your host has indeed a different IP address from the Firewall but is on the same sub-network,
- That the connections are properly in place (use a crossover cable only if you are connecting the Firewall directly to a host or a router. Type "arp -a" in a DOS window under Windows to see if the PC recognizes the Stormshield Network Firewall’s physical address (Ethernet). If it doesn’t, check your cables and the physical connections to your hub…
- That you have not changed the Firewall’s operating mode (transparent or advanced),
- That the Firewall recognizes the IP address (see “How can I check the IP address (es) really assigned to the Firewall?”).
- That the access provider for the graphical interface has not been deactivated on the Firewall.

2) How can I check the IP address (es) really assigned to the Firewall?

If you wish to check the IP address (es) or the operating mode (transparent or advanced) you need only connect to the Firewall in console mode. To do so you can either conduct an SSH session on the Firewall (if SSH is active and authorized) or connect directly to the firewall by the serial port or by connecting a screen and a keyboard to the firewall.

Once connected in console mode (with the admin login) type the command ***ifinfo***. This will give you the network adapter configuration and the present operating mode.

3) What is the meaning of the message 'You lost the MODIFY privilege'?

Only one user can be connected to the Firewall with the MODIFY privilege. This message means that a user has already opened a session with this privilege. In order to force this session to close, you need only connect, adding an exclamation mark before the user's name (!admin).

WARNING

If an administrator session is open on another machine with the MODIFY right, it will be closed.

4) What is the meaning of the message 'The operation has exceeded the allotted time'?

As a security measure any connection between the Firewall and the graphic interface is disconnected after a given time whether finished or not. In particular, this prevents an indefinite wait for a connection if the Firewall cannot be reached via the network.

5) How do I know if there has been an attempted intrusion?

Each attempted intrusion triggers a major or minor alarm, depending on its gravity and configuration. You are informed of these alarms in four ways:

- Firstly the LEDs on the front panel of the firewall light up (red) or flicker (yellow) to alert you.
- Then the alarms are logged in a specific file which you can consult from the graphical interface (**Stormshield Network REAL-TIME MONITOR** or **Stormshield Network EVENT REPORTER**),
- You can receive an alarm report at regular intervals (see *Receiving alarms*) via the Stormshield Network UNIFIED MANAGER application, which can be configured so that whenever an alarm is raised, an e-mail is sent. When several alarms are raised in a short period, they will be sent in a collective e-mail
- Finally **Stormshield Network REAL-TIME MONITOR** displays on the screen the alarms received in real time.

6) It is possible to allow protocols other than IP?

The Stormshield Network Firewall can only analyze IP-based protocols. All protocols that the Firewall does not analyze are regarded as suspicious and are blocked.

However, in transparent mode, Novell's IPX, IPv6, PPPoE, AppleTalk and NetBIOS protocols may be allowed through even though they are not analyzed.

Appendix B: Session and user privileges

Name	Description	Assigned privileges
Logs (R)	Logs consultation	base, log_read
Filter (R)	Filtering policy consultation	base, filter_read
VPN (R)	VPN configuration consultation	base, vpn_read
Logs (W)	Privilege to modify logs configuration	modify, base, log
Filter (W)	Privilege to modify filtering policy configuration	modify, base, filter
VPN (W)	Privilege to modify VPN configuration	modify, base, vpn
Monitoring	Privilege to modify configuration from Realtime Monitor	modify, base, mon_write
Content filtering	Privilege for URL filtering, Mail, SSL and antivirus management	modify, base, contentfilter
PKI	Privilege to modify PKI	modify, base, pki
Objects	Privilege to modify Object database	modify, base, object
Users	Privilege to modify Users	modify, base, user
Network		modify, base, network
Routing	Privilege to modify routing (default route, static routes and trusted networks)	modify, base, route
Maintenance	Privilege to perform maintenance operations (backups, restorations, updates, Firewall shutdown and reboot, antivirus update, modification of antivirus update frequency, High Availability modification and RAID-related actions in Realtime Monitor)	modify, base, maintenance
Intrusion prevention	Privilege to modify Intrusion prevention (IPS) configuration	modify, base, asq
Vulnerability Manager	Privilege to consult or modify vulnerabilities	modify, base, pvm
Objects (global)	Privilege to access to global objets	modify, base, globalobject
Filter (global)	Privilege to access to global filtering policy	modify, base, globalfilter

The *base* privilege is assigned to all users systematically. This privilege allows reading the whole configuration except filtering, VPN, logs and content filtering.

The *modify* privilege is assigned to users who have writing privileges.

The user who has logged on as *admin* will obtain the *admin* privilege. This is the only privilege that allows giving other users administration privileges or removing them.

Appendix C: SA states

-	Undetermined
Larval	The SA is in the process of being negotiated or has not been completely negotiated.
Mature	The SA has been established and is available; the VPN tunnel has been correctly set up.
Dying	The SA will soon expire; A new SA is in the progress of being negotiated.
Dead	The SA has expired and cannot be used; The tunnel has not been set up and is therefore no longer active.
Orphan	A problem has arisen, in general this status means that the tunnel has been set up in only one direction.

STORMSHIELD

documentation@stormshield.eu